

[illegible]

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря Сікорського»**

**ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ
КАФЕДРА ПРОМИСЛОВОЇ ЕЛЕКТРОНІКИ**

«До захисту допущено»
Завідувач кафедри
_____ Ямненко Ю.С.
(підпис) (ініціали, прізвище)
“ ____ ” _____ 20__ р.

**Дипломний проект
на здобуття ступеня бакалавра**

зі спеціальності 6.050802 Електронні пристрої та системи
(код та назва напрямку підготовки або спеціальності)

на тему Охоронна GSM сигналізація

Виконав: студент IV курсу, групи ДС-52
_____ Саларов Михайло Михайлович
(прізвище, ім'я, по батькові)

_____ (підпис)

Керівник _____ доц., к.т.н., доц. Бондаренко О.Ф.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

_____ (підпис)

Рецензент _____ к.т.н. доцент Цибульський Л.Ю.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

_____ (підпис)

Засвідчую, що у цьому дипломному
проекті немає запозичень з праць інших
авторів без відповідних посилань.

Студент _____
(підпис)

Київ - 2019 року

**Національний технічний університет України
“Київський політехнічний інститут
імені Ігоря Сікорського”**

Факультет електроніки
(повна назва)

Кафедра промислової електроніки
(повна назва)

Рівень вищої освіти – перший (бакалаврський)

Напрямок підготовки 6.050802 Електронні пристрої та системи
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Ю.С. Ямненко
(підпис) (прізвище ініціали)

« » 2019 року

**З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ СТУДЕНТУ**

Саларов Михайло Михайлович
(прізвище, ім'я, по батькові)

1. Тема проекту Охоронна GSM сигналізація

Керівник проекту Бондаренко Олександр Федорович, к.т.н доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «25» травень 2019 року № 1404-с

2. Строк подання студентом проекту «11» червня 2019 року

3. Вихідні дані до проекту Охоронна GSM сигналізація.

4. Зміст (дипломної роботи) пояснювальної записки (перелік завдань, які потрібно розробити) Вступ. 1. Аналітичний огляд охоронних сигналізацій. 2. Розробка схеми охоронної сигналізації. 3. Розробка друкованої плати пристрою. 4. Розробка програмного забезпечення.

5. Перелік графічного (ілюстративного) матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо) Схема електрична принципова, схема електрична структурна, складальне креслення.

6. Консультанти розділів проекту

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	Завдання прийняв
1-5			

7. Дата видачі завдання «11» жовтня 2018 року**КАЛЕНДАРНИЙ ПЛАН**

№ з/п	Назва етапів виконання дипломного проекту	Строки виконання етапів проекту	Примітка
1	Аналіз охоронної GSM сигналізації	13.02.2019-08.03.2019	виконав
2	Розробка структурної схеми	9.03.2019-20.03.2019	виконав
3	Розробка друкованої плати	20.03.2019-05.04.2019	виконав
4	Розробка програмного забезпечення	06.04.2019-19.04.2019	виконав
5	Виконання креслень	16.04.2019-01.05.2019	виконав
6	Оформлення пояснювальної записки	05.05.2019-09.06.2019	виконав

Студент

(підпис)

Саларов М.М.

(ініціали, прізвище)

Керівник проекту

(підпис)

Бондаренко О.Ф.

(ініціали, прізвище)

АНОТАЦІЯ

У даному дипломному проєкті було спроектовано та розроблено систему охоронної сигналізації з GSM модулем. Для проектування системи охорони приміщень було прийнято рішення реалізувати даний пристрій на основі МК Arduino Nano. Передача інформацією буде реалізована за допомогою GSM зв'язку, з огляду того що дротові охоронні системи не є надійними. Також GSM зв'язок автоматично робить пристрій незалежним від електрики або Wi – fi модему. Модуль SIM800L допоможе установити GSM зв'язок між нашим пристроєм та оператором мобільного зв'язку.

Після аналітичного огляду, розрахунків було розроблено оптимізовану а найголовніше дешеву систему охоронної сигналізації. Були закуплені відповідні компоненти плати, проведена сборка пристрою та написання програмного коду. Результатом стала до продажу система охоронної сигналізації приміщень, і не тільки.

ABSTRACT

In this diploma project, a security alarm system with a GSM module was designed and developed. To design the system of premises security, it was decided to implement this device on the basis of Arduino Nano MK. The transmission of information will be realized by means of GSM communication, considering that the wired security systems are not reliable. Also, the GSM connection automatically makes the device independent of electricity or a Wi-Fi modem. The SIM800L module will help you establish a GSM connection between our devices and our mobile operator.

After an analytical review, calculations have been developed optimized and the most important cheap security alarm system. The respective components of the card were purchased, the device was assembled and software code was written. The result was the sale of a security alarm system, and not only.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	3
ВСТУП.....	5
Розділ 1. АНАЛІТИЧНИЙ ОГЛЯД ОХОРОННИХ СИГНАЛІЗАЦІЙ.....	6
1.1 Аналіз охоронних GSM сигналізацій	6
1.2 Аналітичний огляд охоронних сигналізацій	10
1.2.1 Структура охоронної сигналізації	10
1.2.2 Види охоронних сповіщувачів.....	11
1.2.3 Периферійні пристрої охоронної сигналізації	17
1.2.4 Живлення пристроїв охоронної сигналізації.....	18
Розділ 2. РОЗРОБКА СХЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ	19
2.1 Розробка схеми електричної структурної.....	19
2.2 Розробка схеми електричної принципової	20
2.3 Вибір елементної бази.....	21
2.3.1 Вибір мікроконтролера.....	22
2.3.2 Вибір GSM модуля	34
2.3.3 Вибір датчику відкриття дверей	43
2.3.4 Вибір п'єзоелементу	43
2.3.5 Вибір понижуючого перетворювача напруги	44
2.3.6 Вибір резисторів	45
2.3.7 Вибір конденсаторів	45
2.3.8 Вибір транзисторів та діодів	46
Розділ 3. РОЗРОБКА ДРУКОВАНОЇ ПЛАТИ ПРИСТРОЮ.....	48
3.1 Вибір друкованої плати.....	48
3.1.1. Вибір типу ДП.....	48
3.1.2. Вибір матеріалу ДП	49

					ДС52.52 17.222.001 ПЗ					
Змн.	Арк.	№ докум.	Підпис	Дата	Охоронна GSM сигналізація. Пояснювальна записка			Літ.	Арк.	Аркушів
Розроб.		Саларов М.М.								
Перевір.		Бондаренко О.Ф.							1	69
Реценз.								КПІ ім. Ігоря Сікорського, ФЕЛ, гр. ДС-52		
Н. Контр.		Батрак Л.М.								
Затверд.		Бондаренко О.Ф.								

3.2 Обґрунтування методу виготовлення ДП	50
3.3 Розрахунок друкованої плати	51
3.4 Проектування друкованої плати в середовищі EasyEda.....	61
Розділ 4. РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	64
4.1 Моделювання програмного забезпечення.....	64
4.1 Програмування контролеру Atmega328P	66
4.3 Тестування програмного забезпечення	67
ВИСНОВКИ	69
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	70
Додаток А. Електрична принципова схема охоронної GSM сигналізації	
Додаток Б. Приклад програми для охоронної GSM сигналізації	
Додаток В. Алгоритм роботи програми	
Додаток Г. Реферат	

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПК – Персональний комп'ютер;

ПІС – Пасивні інфрачервоні сповіщувачі – Passive infrared detectors, PID;

ІЧ – Інфрачервоне випромінювання – Infrared radiation, IR;

АЦП – Аналого – цифровий преобразователь - Analog to digital converter, ADC;

СВЧ – Надвисокочастотне випромінювання – Ultrahigh frequency radiation, UFR;

МК – Мікроконтролер - Micro Controller Unit, MCU;

МП – Мікропроцесор - Microprocessor;

МПК – Мікропроцесорний комплект – Microprocessor kit;

ПЗП – Постійний запам'ятовувальний пристрій – Permanent storage device, PSD;

ОЗП – Оперативно запам'ятовуючий пристрій – Random Access Memory, RAM;

ВІС – Велика інтегральна схема – Large integrated circuit;

РЗП – Регістри загального призначення – General purpose registers;

USB – Universal Serial Bus – Універсальна послідовна шина;

GSM – Global System for Mobile – Глобальна система для мобільних пристроїв;

WLAN – Wireless Local Area Network – Бездротова локальна мережа;

CISC – Complete Instruction Set Computing – Типові архітектурні процесори з повним набором команд;

DIP – Dual Inline Package – Подвійний пакетний рядок;

QFP – Quad Flat Package – Сімейство корпусів мікросхем, що мають планарні висновки, розташовані по всіх чотирьох сторонах;

BOD – Brown out Detector – Вбудована система контролю живлення;

					ДС52.5217.222.001 ПЗ	Арк.
						3
Змн.	Арк.	№ докум.	Підпис	Дата		

FTDI – Future Technology Devices International – Шотландська приватна компанія, яка торгує напівпровідниковими пристроями;

I2C – ІІС – Inter Integrated Circuit – Інтегральна схема;

SPI – Serial Peripheral Interface – Послідовний периферійний інтерфейс;

ШИМ - Широтно імпульсний модулятор – pulse width modulation, PWM;

ISP – In System Programming – внутрішньосхемне програмування;

ISCP – In Circuit Serial Programming – У програмі послідовного циклу;

COM – Component Object Model – Компонентна об'єктна модель;

IDE – Integrated development environment – Інтегроване середовище розробки;

LPT – Line Print Terminal – також паралельний порт, порт принтера;

UART – Universal Asynchronous Receiver Transmitter – Універсальний асинхронний приймач-передавач;

TDMA – англ. Time Division Multiple Access — множинний доступ з поділом за часом;

FDMA – Frequency Division Multiple Access — множинний доступ з поділом каналів за частотою;

GPRS – General Packet Radio Service — пакетна радіозв'язок загального користування;

M2M – Machine to Machine - машинно-машинне взаємодія, загальна назва технологій, які дозволяють машинам обмінюватися інформацією один з одним, або ж передавати її в односторонньому порядку;

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		4

ВСТУП

На даний момент стрімко розвиваються технології, що дозволяють створювати все більше та більше систем, які завчасно попереджають про настання або наближення несприятливої події. Велика кількість життєвих ситуацій, які не завжди викликають посмішку на обличчі. Починаючи від катаклізмів дарованих нам природою, які несуть в собі численні негативні наслідки. Для уникнення несприятливих наслідків людина повинна бути вчасно про інформовану.

У нашому світі саме дуже сильно потрібне оповіщення – це оповіщення про різноманітні природні катаклізми. Але зразу за ним вслід, другим по значущості сповіщенням – є сповіщення про проникнення на територію приватної власності.

Термін GSM в сучасному світі мобільних технологій дозволяє вирішити таке завдання охоронних систем – своєчасно оповістити власника про проникнення на територію приватної власності.

Так склалося, що охоронні системи оснащуються пультами управління, що дистанційно (по радіоканалу) керують охоронні системи. Але якщо цей радіоканал замінити GSM мережею мобільних операторів, а пульти управління – мобільними телефонами, або навіть ПК, підключеними до мережі Internet? Розвиток технологій привів до того що охоронна система має можливість зв'язуватися напряму із телефоном власника по GSM каналу. Відповідно, як управління охоронною системою, так і сповіщення може бути виконано за допомогою смартфона, ПК.

					ДС52.5217.222.001 ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

Розділ 1. АНАЛІТИЧНИЙ ОГЛЯД ОХОРОННИХ СИГНАЛІЗАЦІЙ

1.1 Аналіз охоронних GSM сигналізацій

Ще більше віку тому охоронні сигналізації почали ставати актуальними. Перші прототипи охоронної сигналізації з'явився ще в першій половині IX століття чуть не відразу після винаходу електричного дзвінка. Дуже довгий проміжок часу основним принципом дії охоронної сигналізації було замикання або розмикання контактів або дротяного шлейфу при пошкодженні або спробі проникнути на об'єкт, що знаходився під охоронною.

Ще на початку XX століття великі банки почали застосовувати електричні засоби сигналізації для захисту сейфів та сховищ. Відкриття за відкриттям покращувало роботу охоронних систем.

Доволі швидкий розвиток послуг мобільного зв'язку вплинув на розвиток та поширення охоронних сигналізацій с модулем GSM (Global System Mobile). На відміну від радіосигналу, який є обмеженим по дальності зв'язку, залежить від електропостачання, станції радіосигналу мають доволі великі габарити та енергоємні, GSM джерела мають доволі невеликі розміри (приблизно сучасного смартфона) та не залежать від прямого електропостачання та можуть працювати від звичайного акумулятора. Дальність зв'язку поширення GSM сигналу обмежується тільки особисто вибраним мобільним оператором.

Основна суть охоронної GSM сигналізації полягає у використанні GSM каналу того мобільного оператора, який було обрано користувачем, для отримання або передачі сигналу надсилаючи текстове або голосове повідомлення на мобільний пристрій (смартфон) власника. Дані GSM канали дозволяють про моніторити стан охоронної сигналізації та її параметрів.

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		6

Дуже стисло розглянемо принцип роботи охоронної GSM сигналізації. На об'єкті, який потрібно встановити під охорону, встановлюється спеціальний пристрій (охоронна GSM сигналізація). Даний пристрій оснащений GSM модулем або звичайним мобільним пристроєм (смартфоном). У разі не санкціонованого проникнення на об'єкт контролююча панель активізує GSM модуль та далі можливі такі результати подій: передача текстового повідомлення; виклик на мобільний пристрій власника (смартфон).

У процесі налаштування охоронних GSM сигналізацій в модуль GSM заносять текстові повідомлення, що міститимуть у собі повідомлення про стан охоронної сигналізації та які будуть передаватися на номер телефону, наприклад: «Проникнення до об'єкту», «Відсутність мережі живлення», та багато інших.

Під кожен із подій можна запрограмувати своє унікальне яке нам більш подобається текстове повідомлення. Отримавши текстове повідомлення, власник охоронної GSM сигналізації буде в курсі про стан об'єкта.

Самий найвигідніший (економний) варіант використання охоронної GSM сигналізації. У тому випадку коли на об'єкті виникла «тривога», наприклад, відкриття дверей, вікна під час перебування в режимі охоронна, GSM модуль здійснює дзвінок на номер, що було вказано при налаштуванні. На дисплеї мобільного пристрою буде відображено номер охоронної GSM сигналізації, «піднімати трубку» не обов'язково тому цей варіант вважається найвигіднішим.

На сьогоднішній день оператори мобільного зв'язку пропонують велику кількість різноманітних тарифів без абонентської плати, що автоматично дозволяє не піклуватися про стан мобільного рахунку.

GSM сигналізація – одне з останніх слів в охоронній техніці. Сучасні GSM сигналізації можуть надіслати на мобільний телефон sms повідомлення або додзвонитися і повідомити голосом про проникнення в будинок, квартиру, офіс з приміщення де спрацював датчик, GSM сигналізація дасть вам

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		7

можливість віддалено зі свого мобільного телефону запустити сирену, так само сучасні пристрої GSM охорони і сигналізації своєчасно відправляють сигнал вам і на пульт охорони. GSM сигналізація для авто є досить ефективним засобом охорони. [1]

Склад охоронної GSM сигналізації та поняття про GSM сигналізації розглянемо нижче. Простіше кажучи, це електронний пристрій, в якому є слот, а в деяких моделях навіть кілька (для резервування каналу зв'язку) для установки SIM карти GSM оператора мобільного зв'язку. Хотілося б відзначити, що деякі оператори мобільного зв'язку не підтримують використання таких пристроїв у своїй мережі. Наприклад, Лайф блокує такі сім карти при їх виявленні. У Київстару є спеціальний пакет для GSM сигналізацій - «Датчик». Даний стартовий пакет рекомендовано використовувати, для зменшення витрат. Активізувавши сім карту, для цього треба зробити телефоний дзвінок, на рахунку картки повинні бути кошти, блокування PIN кодом повинно бути відключено. Крім самої центральної плати, тобто GSM модуль, та сім карти, знадобляться допоміжні пристрої, без яких ми не зможемо поставити об'єкт під охорону, включити сирену та інше.

З чого складається GSM сигналізація:

- центральна плата управління, куди вставляється сім карта і підключаються датчики;
- різні охоронні датчики (це і датчики руху, і датчики відкриття дверей, датчики розбиття скла, димові датчики, датчики затоплення, температури і багато інших - залежить від цілей і завдань);
- пристрою постановки / зняття з охорони;
- джерела безперебійного живлення;
- світлозвукові пристрої оповіщення (сирени). [2]

Модуль GSM з різним набором сервісів, який перетворює і передає для користувача системи на приймальне обладнання (мобільний телефон, комп'ютер, центральний пост спостереження, сайт в Інтернеті) сигнали

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		8

тривоги, голосові повідомлення, текстові повідомлення (SMS), технічні параметри яких приймає і перетворює керуючі команди для системи, які вона виконує. Віддалене управління системами і зміна їх режимів роботи можливо за допомогою SMS-повідомлень і DTMF-сигналів, в яких прописуються керуючі команди і які відправляються з мобільного телефону користувача. [1]

Мережа GSM між SIM – картами (телефонними номерами) GSM-модуля і віддаленого Користувача. Якщо користувач системи бажає віддалено здійснювати моніторинг ситуації на об'єкті, реагувати на тривожні сигнали і дистанційно керувати системою - необхідний канал зв'язку. Вибір каналу зв'язку здійснюється з доступного «набору можливостей» на об'єкті. Використовується провідний канал зв'язку, якщо його немає, використовується канал стільниковий зв'язку. Для резервування проходження тривожних і керуючих сигналів від системи можна використовувати два канали - провідний канал і канал стільникового зв'язку. У випадках, коли немає проводів - залишається використовувати тільки канал стільникового зв'язку GSM. При його використанні необхідно враховувати, що даний канал зв'язку підданий ризикам так само, як і провідний. Слабким місцем в каналі зв'язку GSM залишається SIM-карта, носій закритої інформації алгоритму.

Основні плюси використання GSM сигналізації:

- не потрібно платити абонентську плату пульту охорони;
- монтується все швидко;
- на телефон надходять текстові повідомлення або тривожні дзвінки в разі «спрацювання» охоронної сигналізації з деталізацією, що саме спрацювало і де;
- можливість запрограмувати кілька номерів для додзвону;
- крім охоронних функцій, можна контролювати температуру повітря на об'єкті, що охороняється, подія затоплення, управління виконавчими пристроями (включення / вимикання пристроїв);
- економічність.

					ДС52.5217.222.001 ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

Мінуси при використанні GSM сигналізації:

- необхідність самому подбати про «непрошених гостей» у разі спрацювання охоронної сигналізації та захисту приміщення до прибуття поліції;
- залежність надійності зв'язку від мобільного оператора і рівня сигналу [2].

1.2 Аналітичний огляд охоронних сигналізацій

1.2.1 Структура охоронної сигналізації

Структура напряду залежить від самого масштабу завдання, що було поставлено охоронній сигналізації. З цієї залежності впливають такі критерії, які повинні входити до складу обладнання:

- централізоване управління охоронною сигналізацією (ноутбук або персональний комп'ютер на яких було встановлено спеціальне програмне забезпечення, що надає власнику управління охоронною сигналізацією);
- обладнання для обробки та збору інформації з різноманітних датчиків, що використовуються в охоронних GSM сигналізаціях;
- сенсорні пристрої (датчики температури, вологи та сповіщувачі).
- звукові та світлові пристрої сповіщення.

Охоронні GSM сигналізації складаються з різноманітних датчиків, які контролюють об'єкт, який знаходиться під охоронною. При проникненні на об'єкт, що знаходиться під охоронною, видають електричний сигнал. Прилади самостійно не можуть обробити цей сигнал тому застосовують мікропроцесори, що обробляють електричний сигнал та з урахуванням отриманого електричного сигналу визначають подальше виконання дій (надіслати повідомлення на смартфон, подання сигналу тривоги тощо).

					ДС52.5217.222.001 ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2.2 Види охоронних сповіщувачів

Охоронна GSM сигналізація являє собою сукупність різних технічних засобів, модулів, які швидко реагують на зміну параметрів (вторгнення на об'єкт або територію, що охороняється). Найголовнішою задачею перед охоронною сигналізацією стає своєчасне та не помилкове повідомлення власника, поліцію або службу охорони про вторгнення на об'єкт який перебував під охоронною. [21]

Існує так звана залежність способу виявлення «тривоги», всі охоронні GSM сигналізації поділяють три групи:

- адресні охоронні сигналізації, які в повідомленні, що надсилають власнику, містять інформацію про адресу охоронної сигналізації. Дана група дозволяє визначити зону охорони з дуже гарною точністю до місця розташування сповіщувача;
- неадресні охоронні сигналізації сповіщувачі мають деякий, так званий, фіксований поріг чутливості. Група сповіщувачів (два або більше) підключаються до загального шлейфу охоронної сигналізації. У разі спрацювання хоча б одного з групи сповіщувача охоронної сигналізації формується сигнал тривоги;
- адресно – аналогова охоронна система дана група вважається найбільш розвинена та інформативна на відміну від двох попередніх. Основною перевагою над адресними і неадресними системами є застосування сповіщувачів у яких параметри передаються разом з адресою по шлейфу. Адресно – аналогові системи дозволяють, не перериваючи роботу охоронної сигналізації, програмно встановлювати інші параметри сповіщувачів. Даний спосіб моніторингу є найшвидшим у виявленні тривожної ситуації та отримання даних про технічний стан приладу;

Кожна, без виключення, охоронна сигналізація включає в себе один або декілька сповіщувачів. Усі сповіщувачі, які застосовуються в охоронних сигналізаціях розподіляють за типом виявлення тривожних дій:

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

- на рух (інфрачервоні, утразвукові, лінійні та об'ємні магнітоконтатні сповіщувачі);

- на відкриття дверей, вікон тощо (магнітоконтатні);
- на тряску (вібраційні);
- на розбиття скла (акустичні, ударно-контатні);
- на наближення або дотик (ємнісні);
- комбінованими (містять декілька типів одночасно); [4]

Датчики діляться також за способом передачі даних до приладу, наприклад бездротові або дротові. Нижче розглянемо декілька типів сповіщувачів.

Пасивні інфрачервоні сповіщувачі (ПІС) – є одним із найпопулярніших типів сповіщувачів, що використовується в охоронних сигналізаціях. Принципом дії пасивного інфрачервоного сповіщувача ґрунтується на засвідченні змін теплового потоку випромінювання, які створює людина при перетині чутливих зон та перетворення інфрачервоного випромінювання в електричний сигнал. У не складних ПІС сигнал обробляється аналоговим методом, в більш складних цифровим методом за допомогою процесоре. Зона видимості формується спеціальною лінзою «лінза Френеля», яка розсіює лінійний інфрачервоний промінь. Розрізняють об'ємну, поверхневу або лінійну зони виявлення.

ПІС різноманітні за монтажем вони бувають як настільні, так і стельові. Про те саме настінний є найбільш поширеним типом установки. Але дуже не рекомендовано встановлювати ПІС в близькості від дверей, вікон, отворів, де формуються повітряні потоки та джерел які виробляють тепло. Також ПІС чутливі на світлове випромінювання від ламп, сонцю. Деякі інфрачервоні сповіщувачі не можна ставити у приміщення де є кішка або інша домашня тварина. У такому випадку використовують ПІС зі спеціальними лінзами в яких існує захист від домашніх тварин [22].

На рис. 1.1 представлено ПІС моделі «Crow GENIUS».



Рис. 1.1

На рис. 1.2 представлена діаграма зони виявлення ПІС зі спеціальними лінзами, які потрібні для захисту від виявлення домашніх тварин.

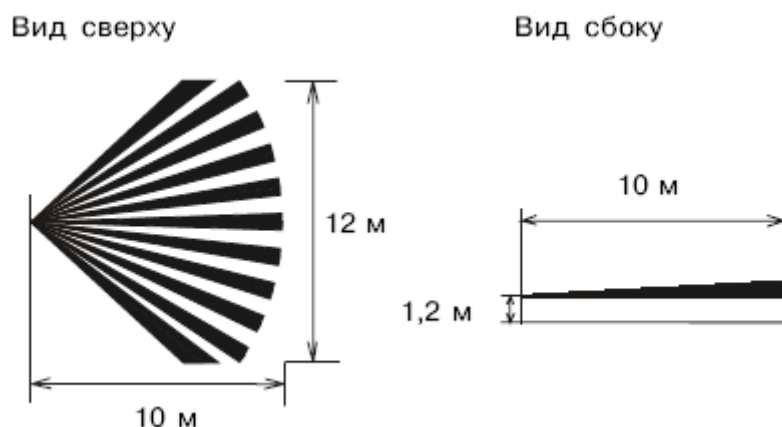


Рис. 1.2

Інфрачервоні активні сповіщувачі – так названі оптичні системи з ІЧ – приймача та ІЧ – випромінювача. Площу яку може охоплювати інфрачервоний активний сповіщувач своїм «оком» досягає близько 100 метрів. Саме цей тип сповіщувачів використовуються для об'єктів з великою площею, наприклад зовнішнього кордону. Принципом дії інфрачервоного активного сповіщувача оснований на формуванні імпульсного ІЧ

випромінювання випромінювачем, що в свою чергу приймає приймач ІЧ випромінювання.

Однією з переваг даного сповіщувача є можливість регулювати час переривання променів, налаштовувати під особливості різних об'єктів. Якщо встановити великий час переривання сповіщувач буде виявляти порушників та пропускати котів, собак, птахів. Дана перевага дозволяє збільшити стабільність роботи системи.

Розрізняють два типу ІЧ активних сповіщувачів: однопроменевими так і багатопроменевими. Якщо кількість променів більша як два тоді зменшується поява помилки це пояснюється тим що сигнал тривоги відбувається при перетині всіх променів одночасно. [22]

На рис. 1.3 представлено модель інфрачервоного активного сповіщувача «SELCO SBQ-150S».



Рис. 1.3

Магнітоконтатні сповіщувачі (МС) – цей сповіщувач досить часто можна зустріти на дверних та віконних прорізах. Основне призначення магнітоконтатних сповіщувачів є блокування віконних або дверних прорізів. Даний сповіщувач складається з магнітокерованого датчика на основі магніту та геркону. Основною відмінністю МС один від одного є тип установки, з

якого матеріалу виготовлені. Економічні, мають дешеву ціну на ринку з порівнянням з другими сповіщувачами. [23]

На рис. 1.4 представлено модель магнітоконтального сповіщувача СМК.



Рис. 1.4

Ударно контактні сповіщувачі – принципом дії базується на засвідченні розмикання рухомих контактів датчика вібрації, руйнування скляного полотна. Не рідко даний сповіщувач можна побачити на вітринах у магазині або вікнах. Саме ударно контактний сповіщувач фіксує руйнування скляного полотна різного за товщиною. Ударно контактні сповіщувачі стійкі до низькочастотних коливань, що припадають на поверхню скла, наприклад грім, легкий землетрус, гуркіт.

Розглянутий сповіщувач фіксує появу декількох його складових поздовжніх і поперечних високочастотних коливань скляного полотна при його руйнуванні. [23]. На рис. 1.5 представлено ударно контактний охоронний сповіщувач «Вікно – 6».



Рис. 1.5

Акустичні охоронні сповіщувачі – виявляють руйнування листових дзеркал. Акустичний охоронний сповіщувач містить чутливий елемент електричний конденсаторний мікрофон із підсилювачем на польовому транзисторі. Сам принцип роботи полягає у перетворенні мікрофоном звукових коливань повітряного середовища в електричний сигнал, а саме з електричного сигналу надходить на підсилювач та далі на МК. Мікроконтролер у свою чергу із урахуванням заданої йому програми виробляє контроль акустичних сигналів, напруги живлення та формування відповідних повідомлень.

При установці акустичного охоронного сповіщувача слід враховувати, що всі ділянки повинні бути в межах його видимості. [23]

На рис. 1.6 представлено модель акустичного охоронного сповіщувача.



Рис. 1.6

Вібраційні сповіщувачі – дані сповіщувачі використовують для захисту банкоматів, сейфів від проникнення шляхом руйнування стін, різних перекриттів. Принцип дії вібраційного сповіщувача базується на основі п'єзоелектричного ефекту, що являє собою зміну електричного сигналу, яка здійснюється при зміні вібрації п'єзоелемента. Однією із характеристик вібраційного сповіщувача є чутливість до вібрації. Посилення вібрації призводить до посилення електричного сигналу (пропорційність) та обробляється схемою самого сповіщувача.

На рис. 1.7 наведений приклад сповіщувача, який застосовують для захисту банкомату за допомогою сповіщувача вібраційного сповіщувача.



Рис 1.7

1.2.3 Периферійні пристрої охоронної сигналізації

Усі пристрої які використовуються в охоронній сигналізації без виключення, окрім сповіщувачів, вважаються периферійними пристроями. Тобто це пристрої, що мають власне конструктивне виконання та під'єднуються до контрольної панелі охоронної сигналізації за допомогою зовнішньої лінії зв'язку. Дуже часто в охоронних сигналізаціях можна помітити такі типи периферійних пристроїв:

- пульт управління – використовують для управління охоронними сигналізаціями;
- модуль для запобігання коротких замикань – використовується для забезпечення працездатності охоронної сигналізації, якщо станеться коротке замикання;
- модуль входу та виходу – використовується для управління зовнішніми пристроями та контролю цих пристроїв;

- модуль підключення неадресної лінії – використовують для управління та контролю неадресних сповіщувачів, які є в наявності охоронній системі;
- релейний модуль – використовують для управління контрольною панелі охоронної сигналізації також допомагає розширити функції сповіщення;
- звуковий сповіщувач – використовують для сповіщення про «тривогу» у разі необхідності, проникнення до об'єкта, сповіщення здійснюється за допомогою звукової сигналізації;
- світловий сповіщувач – використовують в таких самих цілях, що і звуковий сповіщувач;
- принтер повідомлень – використовують для друку тривожних або службових системних повідомлень; [3]

1.2.4 Живлення пристроїв охоронної сигналізації

Для автономної роботи охоронної сигналізації все пристрої без виключення повинні бути забезпечені безперебійним електроживленням. Охоронна сигналізація в якості основного, за частіше, використовують так зване мережеве електроживлення. За часту вони живлять контрольну або управляючі панелі охоронної сигналізації. Усі інші пристрої охоронної сигналізації живляться від низьковольтних вторинних джерел постійного струму. Згідно вже встановленим нормам охоронної безпеки, кожна охоронна сигналізація повинна мати автономне джерело живлення, для безперебійного функціонування. У разі відключення від мережевого електропостачання охоронна сигналізація повинна функціонувати хоча б протягом доби в так званому «черговому» режимі. Щоб виконати цю вимогу охоронні сигналізації оснащують резервним електроживленням. Додаткові або вбудовані акумулятори також можна використовувати супер конденсатори, які накопичують достатньо енергії для живлення охоронної сигналізації. [3]

РОЗДІЛ 2. РОЗРОБКА СХЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ

2.1. Розробка схеми електричної структурної

Структурна схема охоронної сигналізації повинна складатися із декількох частин:

- функціональний блок до складу якого входить МК та різні датчики;
- пристрій моніторингу та керування (смартфон або персональний комп'ютер зі встановленим спеціальним програмним забезпеченням або віддалений сервер за допомогою якого можна моніторити та керувати охоронною сигналізацією;

Структурна схема пристрою складається з функціонального блока до складу котрого входить:

- блок живлення;
- понижуючий перетворювач напруги LM2596;
- GSM модуль SIM800L;
- датчик відкритих дверей МС-38;
- МК;
- динамік;
- блок індикації, світлодіод;

Структурна схема дає уявлення про зв'язок між окремими модулями, але не відображає окремі мікроборки, що утворюються при об'єднанні певних блоків.

Для обміну даними між функціональним блоком та користувачем будемо використовувати сервер, який буде проміжним місцем збереження даних при роботі модуля та інтерфейсу користувача.

Периферійні пристрої підключені до МК за допомогою цифрових виводів. Електропостачання буде здійснюватися від джерела живлення.

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

Враховуючи характеристики GSM модуля його живлення здійснюється за допомогою понижуючого перетворювача напруги.

На рис. 2.1 зображена схема електрична структурна охоронної сигналізації с GSM модулем.

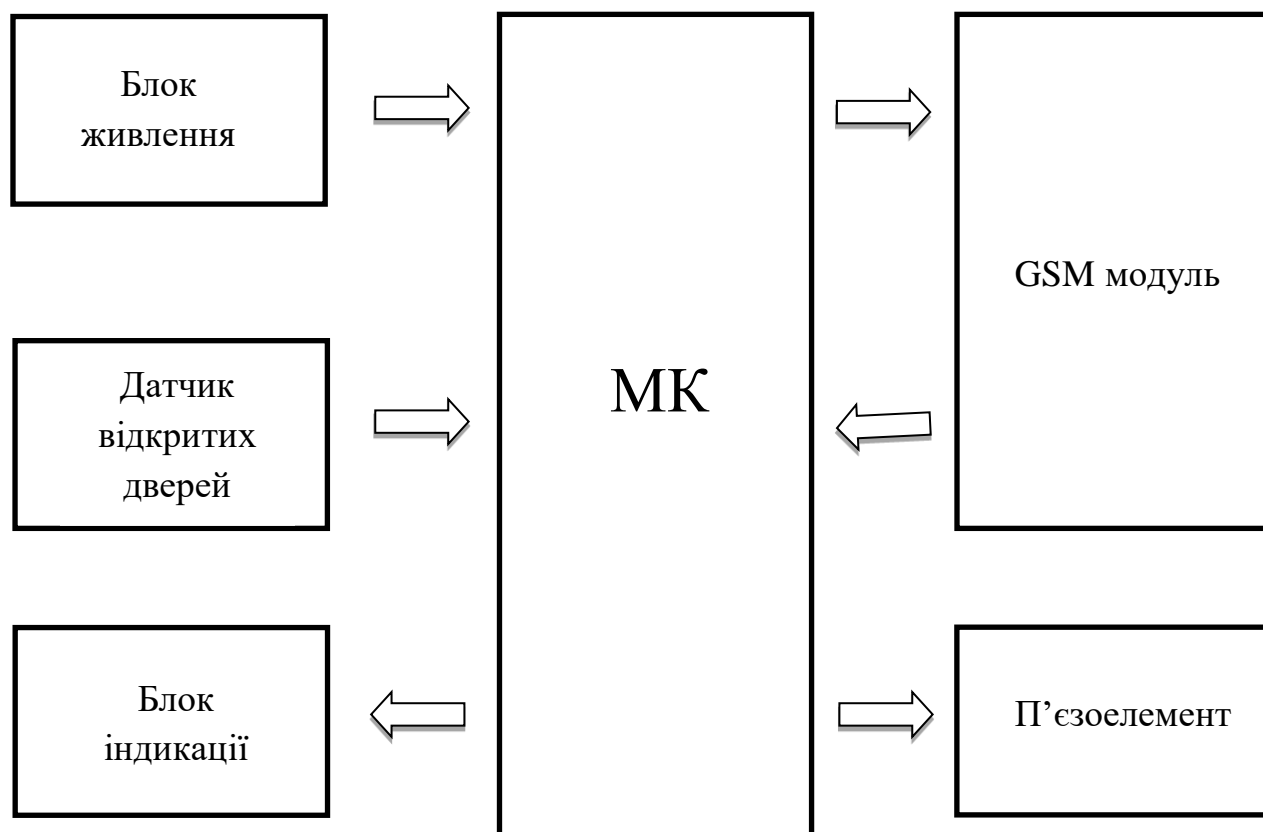


Рис. 2.1

2.2. Розробка схеми електрично принципової

Схема електрична принципова охоронної GSM сигналізації повинна виконувати всі функції, які поставлені перед охоронною GSM сигналізацією. Виходячи з цього, розглянемо блоки пристрої, що виконують свої функції та перебувають у взаємозв'язку між собою.

Схема живлення

У ході розробки схеми живлення було спроектовано систему, котра буде живитися від блоку живлення у 9В, а коли блоку живлення не має, або зникає напруга, система починає працювати від двох Li-Po акумуляторів типу 18650. Тому при підключеному блоці живлення ці акумулятори необхідно заряджати. Для цього у схему було добавлено блок контролю заряду, балансир напруги двох акумуляторів, індикатори заряду та розряду акумуляторів.

Контроль заряду та балансир напруги побудовані на двох польових транзисторах. Коли один акумулятор має більшу напругу, ніж інший, польовий транзистор зачиняється, та до нього перестає йти струм. Коли напруги акумуляторів вирівнюються, транзистор відчиняється і блок живлення знову заряджає обидва акумулятори. Це зроблено, щоб збільшити час напруцювання батарей. Для живлення GSM модуля використано понижуючий перетворювач напруги, який понизує напругу до 4 В.

Схема керування

В основі системи керування лежить мікроконтролер Atmega328P. Приймаючи сигнал від модулю або від підключеної периферії він обробляє його і формує інструкцію.

У ході розробки електричної принципової схеми охоронної GSM сигналізації. Було розроблено електрично принципову схему яка зображена у додатку А.

2.3 Вибір елементної бази

Основними вимогами, якими потрібно керуватися при проектуванні радіоелектронної апаратури, є вимоги його високої надійності, швидкості роботи, оптимальна вартість приладу та мінімальні малогабаритні показники. Крім того, при проектуванні важливо використовувати переважно цифрові

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		21

мікросхеми, так як вони дають більшу швидкість роботи схеми, її компактність, меншу похибку при вимірюваннях (для вимірювальних пристроїв), спрощують виробництво. Виходячи з перерахованих вище критеріїв, зробимо вибір елементної бази.

2.3.1 Вибір мікроконтролера

Найважливішим рішенням є вибір МК, від якого на пряму буде залежати, як добре буде функціювати охоронна сигналізація. Треба враховувати велику низку факторів, які вплинуть на працездатність та швидкодію охоронної сигналізації. Швидкий розвиток мікропроцесорної техніки приводить на ринок великої кількості асортименту даної продукції.

Основною перевагою використання МК є те, що за допомогою МК можна конструювати велику кількість різних пристроїв, які не будуть великогабаритними, дорого коштуючи ми та будуть надійними та сумісними із мобільними пристроями (смартфонами) та персональними комп'ютерами через стандартні інтерфейси.

Мікропроцесор (МП) – це пристрій, який здійснює приймання, обробку і видачу інформації. Конструктивно МП містить одну або кілька інтегральних схем і виконує дії за програмою, яка зберігається в його пам'яті.

Мікроконтролер (англ. Micro Controller Unit, MCU) – мікросхема, призначена для управління електронними пристроями.

Типовий МУ поєднує на одному кристалі функції процесора та периферійних пристроїв, містить ОЗП або ПЗП. По суті, це одно кристальний комп'ютер, здатний виконувати досить прості завдання.

За основу розробки охоронної сигналізації була поставлена мета зробити її не дорогою тому МК вибираємо найменш дорогий, але який буде задовольняти всі наші вимоги, а саме:

- надійність;
- малогабаритність;

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		22

- продуктивність;
- умови застосування;

Пошук МК який буде задовольняти нашим вимогам буде включати в себе підбір відповідної літератури про різні типи МК та порівняльна характеристика. Вибір прикладної мови на якій буде здійснено програмування (наприклад, С або С++) дуже сильно може вплинути на продуктивність, швидкодію охоронної сигналізації.

Виробники МК дуже різні цим займаються багато фірм таких як: Intel, MicroChip, Atmel, Phillips, Siemens та інші. Але нашої уваги заслуговують не всі фірми, розглянемо декілька фірм по виробництву МК Intel, MicroChip, Atmel.

Кожна із перелічених вище фірм мають широку номенклатуру МК, які виконують задачі управління та мають в собі набори вузлів обробки, зберігання даних. Обрані периферійні, які будуть підключені до МК, допоможуть більш ефективно вирішити поставлені задачі. Треба провести детальний порівняльний аналіз за багатьма параметрами, щоб визначити який МК краще використовувати. У табл. 2.2 наведені параметри МК виробників: Intel - 8051, 8751; MicroChip - PIC 16C57, PIC16C71; Atmel - AT90S8515, ATmega 603.

МК фірми Intel – це CISK – процесори (complex instruction set computing или complex instruction set computer), дані МК мають доволі складну систему з різними типами адресації, складний пристрій управління та невелику кількість регістрів загального положення (РЗП).

МК фірм MicroChip та Atmel будуються іншою архітектурою. Ядро цих МК – це RISK – процесор, який має доволі просту систему команд, які однакові за форматом та здійснюють, в основному, операції типу регістр - регістр. такі процесори мають велику кількість РЗП. Дана особливість, будови архітектури майже дозволяє виконувати всі команди, окрім команд програмних переходів, за один машинний цикл, і машинний цикл займає значно менше тактів – у

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

контролерів PIC – 4 такти, у МК Atmel – 1 такт. При однаковій частоті продуктивність МК буде вища в декілька разів. [9]

Таблиця 2.2

	Intel		MicroChip		Atmel	
	8051	8751	PIC16C57	PIC16C71	ATmega603	AT90S8414
Система команд	111	111	33	35	121	120
Програмна пам'ять	4Kx8 ROM	4Kx8 EPROM	1Kx12 EPROM	8Kx14 EPROM	64Kx16 Flash	8Kx16 Flash
Пам'ять даних	128 x 8 SRAM	128 x 8 SRAM	80 x 8 REG	36 x 8 REG	4K x 8 SRAM, 2K x 8 EEPROM	256x8 SRAM, 256 x 8EEPROM
Тактова частота	3,5..12 МГц	3,5..12 МГц	0..20 МГц	0..20 МГц	0..6 МГц	0..20 МГц
Інтерфейс	UART	UART	-	-	UART + SPI	UART+SPI
Захист пам'яті	-	-	+	+	+	+
Система переривань	+	+	+	+	+	+
Аналоговий компаратор	-	-	-	-	+	+
АЦП	-	-	-	-	+	+

Фірма Intel при виробництві своїх МК використовує технологію NMOS, а фірми MicroChip і Atmel - CMOS - технологію. Ці технології обидві є МОП – технологіями. Але перевага надається CMOS технології, тому що вона дозволяє знижену напругу живлення до 2,5 – 2,7 при одній і тій же потужності, що розсіюється використовувати біль високу тактову частоту. МК типу PIC та Atmel мають доволі широку межу живлення напруги та мають енергозберігаючі режими функціонування, також вони можуть працювати на частотах близьких до 0 Гц. Це дозволяє зменшити значення протікаючого струму в низько швидкісних режимах. [10]

З розглянутих основних особливостей зрозуміло, що МК фірми Intel значно поступаються МК фірмам PIC і Atmel в якісних показниках. Тому МК фірми Intel з подальшого аналізу ми виключаємо та будемо проводити аналіз тільки PIC та Atmel.

Детальніше розглянемо кількість команд фірми Atmel, команди даного МК дозволяють зменшити довжину написаного коду. Дії МК Atmel можуть виконуватись однією і тією ж командою на відмінну від МК PIC. Логічні та арифметичні операції МК Atmel виконується між двома регістрами, а у МК PIC потребує використання так званого регістра – акумулятора. МК Atmel мають більш широке коло операцій з окремими бітами регістрів. Данна особливість робить код програми Atmel менше, ніж PIC, а отже, вона займає менше програмної пам'яті, та менше час її виконання. Порівняння команд Atmel і PIC наведені в табл. 2.3 [11]

Таблиця 2.3

Atmel	Циклів	тактів	PIC	слів	циклів	тактів
ADC R4,R5	1	1	BTFSB 0x03,0 INCF 0x05 ADDWF 0x04,1	3	3(4)	12(16)
SUB R4,R5	1	1	MOVF 0x04 SUBWF 0x05 MOVWF 0x04	3	3	12
AND R4,R5	1	1	MOVF 0x05 ANDWF 0x04,1	2	2	8
ORI R4,K	1	1	MOVF 0x04 IORLW K MOVWF 0x04	3	3	12
CLR R4	1	1	MOVF 0x04 XORWF 0x04,1	2	2	8
JMP A	2	3	GOTO A	1	2	8
CALL A	2	4	CALL A	1	2	8

З порівняльної табл. 2.3 випливає перевага Atmel над PIC, які в свою чергу вимагають виконання команд пересилань.

Зберігання програми МК Atmel відбувається у спеціальній незалежній пам'яті. МК PIC в старих версіях зберігає програми в ROM пам'яті, а в більшій кількості моделей в EPROM. Зберігання МК Atmel у спеціальній незалежній пам'яті є однією з головних переваг. Flash пам'ять перезаписується напругою в робочому діапазоні МК, що дозволяє виробляти внутрішньо схемне програмування МК, тобто виймання його зі схеми, для чого в МК Atmel

передбачений послідовний SPI інтерфейс, через який можна перепрограмувати пам'ять програм МК, наприклад від ПК. [10]

Дані у Atmel і у PIC розміщуються в невеликій за обсягом SRAM, але крім неї Atmel має EEPROM для даних, що дозволяє зберігати постійні параметри для роботи програми. [11]

У результаті проведення аналізу фірм, що виробляють МК була виявлена переваги фірми Atmel.

Вибір плати МК із урахуванням порівняльних характеристик

Основною метою було поставлено вибрати найменш дорогий МК, який буде повністю задовольняти поставлені вимоги охоронної сигналізації. Із найпопулярніших плат фірми Atmel було обрано плату Arduino Nano, яка входить до трійки най популярніших плат, які використовують для створення різноманітних пристроїв. Дану плату доречно використовувати в різних проектах де основними критеріями є ціна та компактність.

Плата Arduino Nano працює на чіпі ATmega328P (хоча можна ще зустріти плати на основі чіпа ATmega168). [13]

Опис чіпу ATmega328P

Мікроконтролер ATmega328P є 8-ми розрядним CMOS МК з низьким енергоспоживанням, заснованим на вдосконаленій AVR RISC архітектурі.

ATmega328P – мікроконтролер сімейства AVR, як і всі інші має 8-бітний процесор і дозволяє виконувати більшість команд за один такт. [12]

Кожен мікроконтролер серії, від найперших, наприклад, Atmega3, до найбільш сучасних (Atmega328 або Atmega2561 rev3), характеризується повністю статичними темпами роботи.

Дуже велика продуктивність, що затверджена в описі чіпу. Згідно з описом при частоті в 16 мегагерц продуктивність буде приблизно дорівнювати 16 мільйонам операцій за 1 секунду. [14]

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

Існує декілька варіантів в якому корпусі виготовляються даний чіп. На рис. 2.4 Atmega328P в корпусі PDIP та 2.5 Atmega328P в корпусі TQFP зображено розташування виводів чіпу для різних типу корпусів.

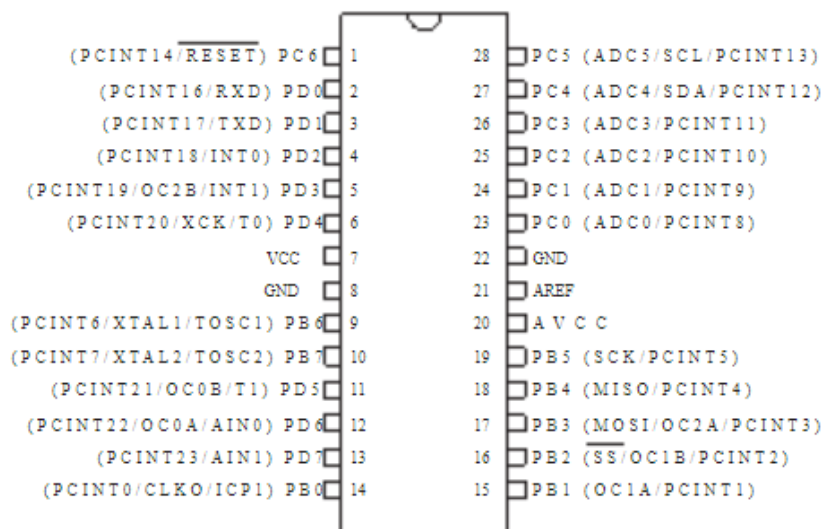


Рис. 2.4

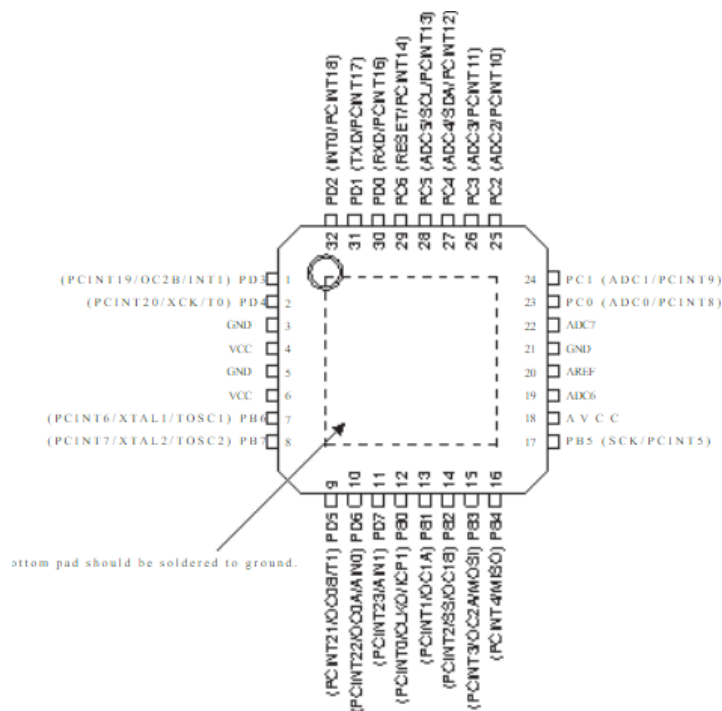


Рис. 2.5

DIP (Dual Inline Package) – це корпус із двома рядами контактів для впайки в отвори в друкованій платі. Даний корпус має прямокутну форму розташованими на сторонах контактами. У залежності від матеріалу виготовлення корпусу виділяють на дві підгрупи:

- PDIP (Plastic DIP) – пластиковий корпус;
- CDIP (Ceramic DIP) – керамічний корпус.

QFP (Quad Flat Package) – це плоский корпус, який містить чотири ряди контактів, що потрібні для поверхневого монтажу. Даний корпус має квадратну або прямокутну форму. У залежності від матеріалу виготовлення корпусу виділяють на дві підгрупи:

- PQFP (Plastic QFP) – пластиковий корпус;
- CQFP (Ceramic QFP) – керамічний корпус.

На рис. 2.6 зображена блок схема чіпу Atmega328P. [15]

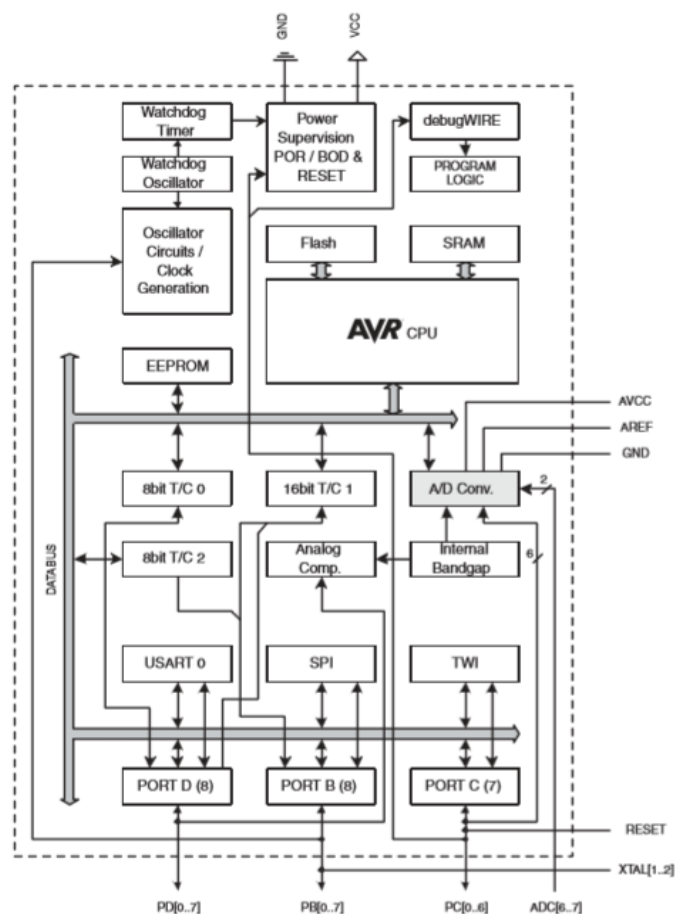


Рис. 2.6

Особливості ATmega328P

Atmega328P порівняно з Atmega328 споживає менше енергії, що означає, що для Atmega328P використовувався більш точніший технічний процес (60 нм у ATmega328P проти 90 нм у ATmega328). Якщо порівнювати ціну чіпів, то чіпи Atmega328P зазвичай дорожчі. ATmega328P краще використовувати у спеціальному режимі управління живленням для зниження енергоспоживання пристрою.

Atmega328P доступний корпус типу TQFP32, що не можна сказати про Atmega328. Скоріш за все це зв'язано з товщиною кристала у чіпа Atmega328, товщина кристала більше, та він банально не поміщається в корпус TQFP32.

У Atmega328 відсутній фізюз для заборони детектор не якісного джерела живлення BOD (Brown-out Detector), а у Atmega328P цей фізюз присутній, це автоматично дозволяє зменшити енергоспоживання.

Існують доволі незначні відмінності в системі команд. Якщо написати програму для чіпу ATmega328P, вона не завжди буде працездатна для чіпу ATmega328P. [24]

Вибір плати Arduino

Arduino Nano – вважається аналогом плати Arduino Uno, яка до речі також працює на чіпі ATmega328P, основна їхньою відмінністю є формфактор плати, яка у плати Nano приблизно в 2 – 2,5 менша за Uno. Розміри плати Uno подібні пачці сигарет та дозволяють легко збирати прототипи різних схем навісним монтажем. Але для зменшення габаритів приладу доречно використовувати плату Nano. [17]. На рис. 2.7 зображено Arduino Uno та Nano.

Одна з відмінностей плати Nano, полягає у відсутності гнізда, через яке здійснюється зовнішнє живлення плати, але цей недолік вирішується шляхом установлення на друковану плату спеціального гнізда та підключення його к виводам плати.

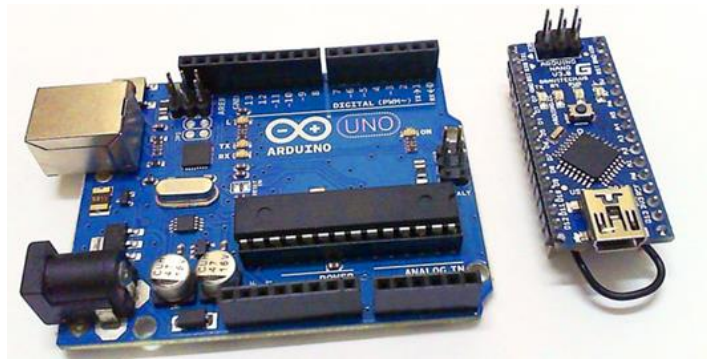


Рис. 2.7

Зв'язок з різними пристроями, периферіями здійснюється за допомогою інтерфейсів UART, I2C і SPI. На рис. 2.8 зображено плату Arduino Nano.

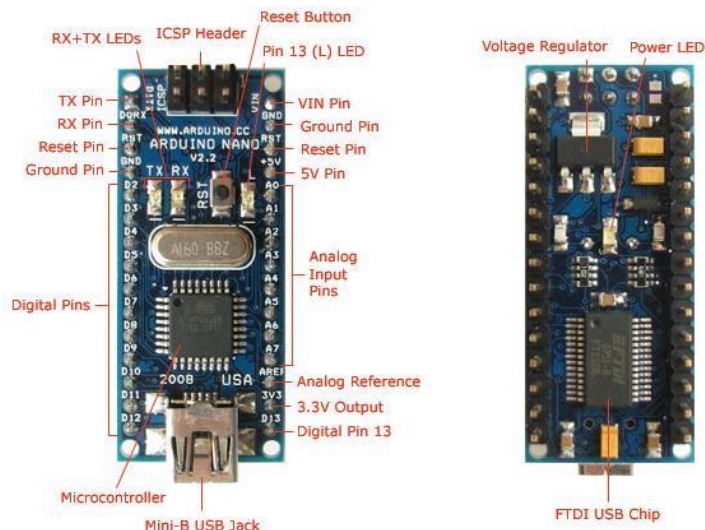


Рис. 2.8

Технічні характеристики Arduino Nano наведені в табл. 2.9.

Треба відзначити, що виробник плат Arduino Nano випускає дану плату в декількох версіях. Найпоширенішими вважаються версії Nano v.2 та Nano v.3. Головна відмінність у версіях це відмінність чіпів для версії Nano v.2 це Atmega168, а для Nano v.3 це Atmega328. Тим самим відмінність чіпів вказує на різницю обсягу Flash пам'яті.

Плата Arduino Nano є не най компактнішою платою головним конкурентом в розмірах є Arduino micro. Nano та micro дуже сході але у micro

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		30

змінена кількість переривань та інтерфейси SPI, I2C розлучені на інші піни порівняно з Nano.

Таблиця 2.9

Мікроконтролер Atmel ATmega168 або ATmega328	
Робоча напруга (логічний рівень)	5 В
Вхідна напруга (рекомендована)	7-12 В
Вхідна напруга (гранична)	6-20 В
Цифрові Входи / Виходи	14 (6 з яких можуть використовуватися як виходи ШІМ)
Аналогові входи	8
Постійний струм через вхід / вихід	40 мАх з одного виводу і 500 мАх з усіх висновків
Флеш пам'ять	16 Кб (ATmega168) або 32 Кб (ATmega328) при цьому 2 Кб використовуються для завантажувача
ОЗУ	1 Кб (ATmega168) або 2 Кб (ATmega328)
EEPROM	512 байт (ATmega168) або 1 Кб (ATmega328)
Тактова частота	16
Розміри	1.85 см x 4.2 см

Плата Arduino Nano має чотирнадцять цифрових входів з яких шість можуть працювати як ШІМ, вісім аналогових входів, які також можна використовувати як цифрові виходи, два вивода задіяні під I2C та три під SPI.

На одному з кінців плати розташована «колодка» ICSP, що служить для прошивки МК плати через ПК.

За допомогою ШІМ виходів можливо регулювати о

Цифрові виходи 2 та 3, якщо це потрібно, можуть бути використані для зовнішніх сигналів переривань. За цим сигналом викликається спеціальна програма обробки переривань, що виконує спеціальні дії. Наприклад вихід з режиму енергозбереження та засвідчення зеленого світлодіоду.

Живлення плати здійснюється за допомогою mini – USB або micro – USB при підключенні до комп'ютера або через зовнішнє джерело живлення в діапазоні напруги 6 – 20 В. [17]

В даній платі є обмеження по струму та напругу на входах та виходах плати. Усі виходи (цифрові та аналогові) працюють в діапазоні 0-5 В. Якщо

подавати живлення вище заданого діапазона, то така напруга буде обмежуватися діодами, стабілізаторами. Такий випадок змушує сигнал бути підключеним через резистор інакше плата вийде з ладу. На входи не повинен потрапляти струм більше за значення 40 мА.

На рис. 2.10 зображено розташування контактів на платі Arduino Nano версії 3.0.

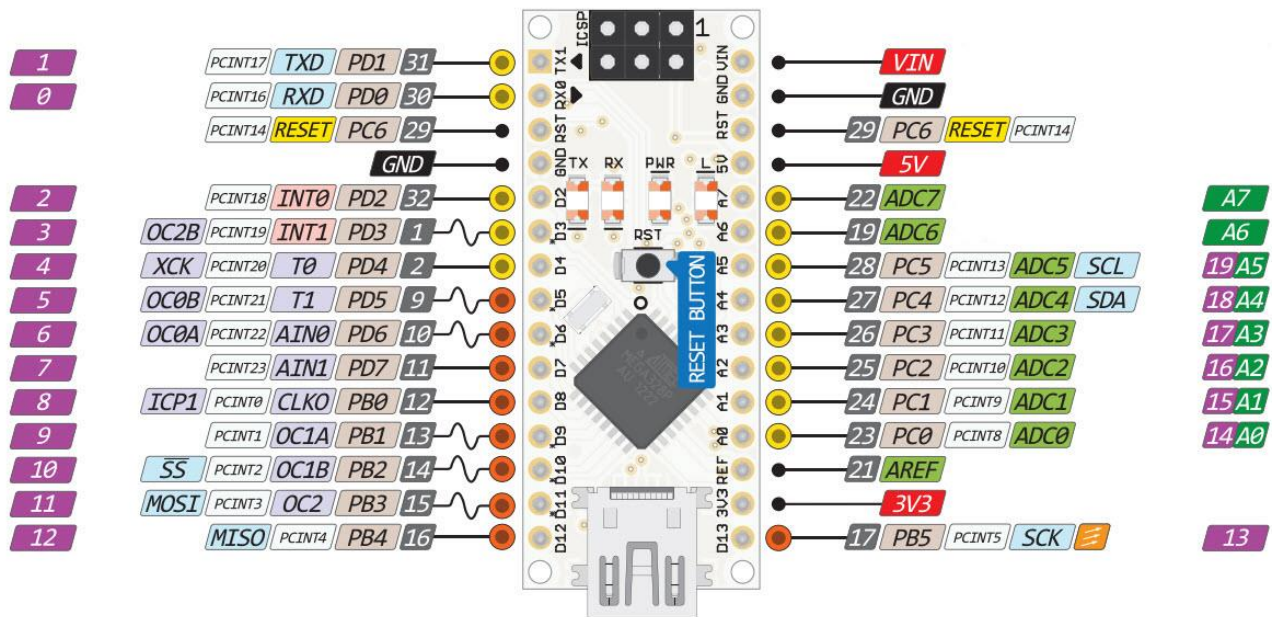


Рис. 2.10

Цифрові контакти позначаються англійською літерою D, може бути як входи так і виходи та на кожному з них є підтягуючий резистор, що можна підключати програмно. Аналогові контакти позначаються англійською літерою A і використовуються як входи. На аналогових контактах відсутні підтягуючі резистори.

На 6 цифрових контактах можна побачити значок тильди «~». Такі контакти використовуються в якості ШІМ. Для використання ШІМ в програмі треба вказати спеціальну функцію `analogWrite()`. [18]

Для програмування контролерів фірми Atmel, треба підключити програматор, для цього використовують спеціальний інтерфейс ICSP.

На рис. 2.11 зображена принципова електрична схема плати Arduino Nano.

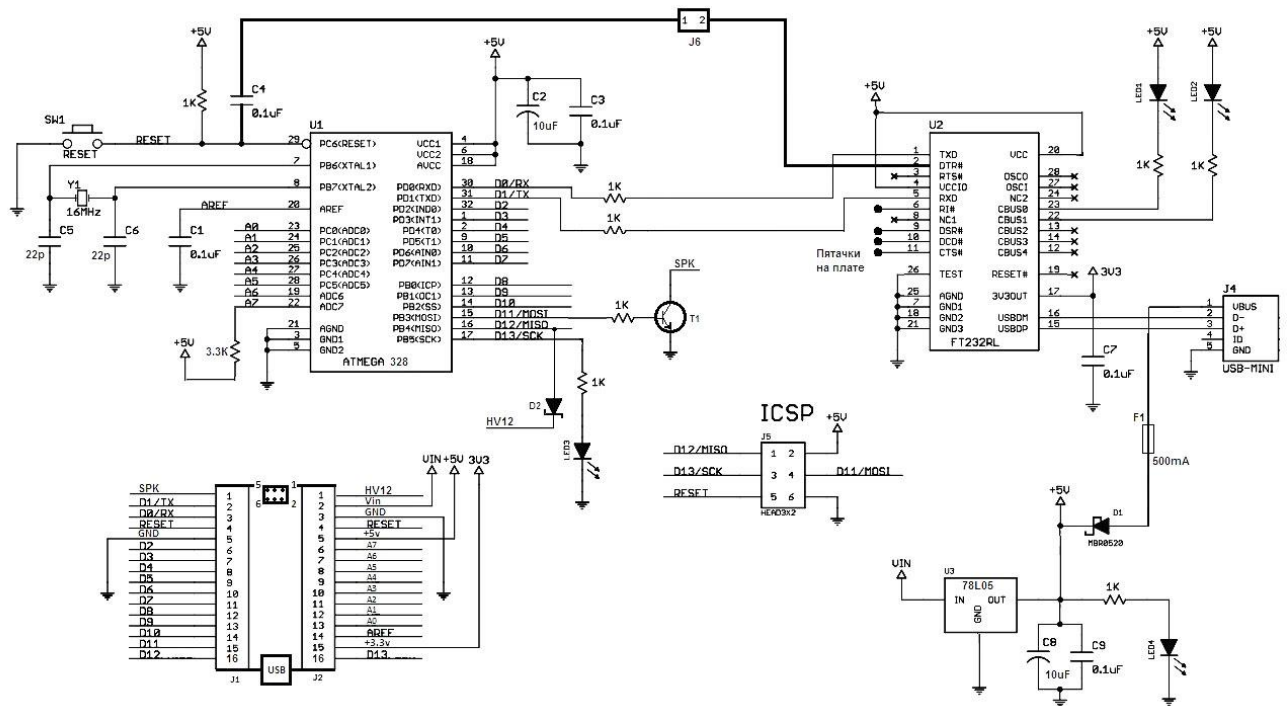


Рис. 2.11

Для плати Arduino Nano інтерфейс ICSP знаходиться на контактах які зображені на рис. 2.12, де

- 1 - MISO (провідний приймає від веденого);
- 2 - + 5V (живлення);
- 3 - SCK (тактовий імпульс);
- 4 - MOSI (провідний передає відомому);
- 5 - RESET (скидання);
- 6 - GND (земля);

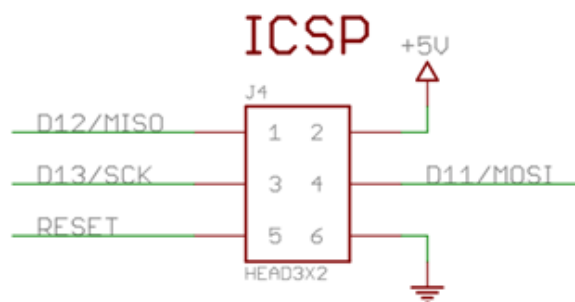


Рис. 2.12

Один із 6 контактів роз'єму виглядає у формі квадрату. Нумерація починається за годинковою стрілкою. Прошивка контролера змінюється за допомогою спеціального середовища програмування та кабелю USB. Покупка програматору стає непотрібна, що допомагає з економити кошти [17].

Налаштування Arduino IDE для програмування Arduino Nano

Для написання програм для плат Arduino використовують спеціальне середовище, яке має назву Arduino IDE.

Arduino IDE – це програмне середовище розробки, призначена для програмування плат Arduino. На сьогоднішній день за допомогою плат Arduino створюють різні пристрої, навчальні моделі та багато іншого. Інтерфейс середовища розробки доволі просте, зрозумілий навіть по силі дитині. За основу програмного середовища лягла мова C++, саме середовище було створено за допомогою мови програмування Java. [25]

Для початку роботи з програмним середовищем розробки Arduino IDE її потрібно завантажити з офіційного сайту, завантаження виконується безшкотовно. Після завантаження програми переходимо до процесу установки її на ПК. Запустивши Arduino IDE на своєму ПК потрібно підключити плату до ПК за допомогою USB. Та перейти до написання потрібної програми. На верхній панелі треба обрати вкладку «інструменти» та вибрати плату, в даному випадку Arduino Nano, та обрати порт до якого підключена плата. [18]

2.3.2 Вибір GSM модуля

GSM (від назви групи Groupe Special Mobile, пізніше перейменований в Global System for Mobile Communications) – так званий глобальний стандарт цифрового мобільного зв'язку із розподіленням каналів за частотою та часом.

Використання GSM модулів дозволяє підключатися та надсилати команди через звичайний мобільний зв'язок. Відправляти та приймати команди на пристрій здійснюється за допомогою SMS – команд або через інтернет – підключення.

GSM модуль допомагає платам Arduino розширити свої можливості таких як: відправка текстових або голосових повідомлень, здійснення дзвінків. Існує велика кількість GSM модулів проаналізувавши ринок були виділено такі модулі: SIM900, SIM800L, A6, A7. [27]

Для вибору GSM модуля про аналізуємо та проведемо порівняльну характеристику.

Опис модуля SIM900

GSM модуль SIM900 використовують в різноманітних автоматизованих системах. За допомогою такого інтерфейсу, як UART здійснюється передача даних між пристроями. Даний модуль допомагає здійснювати обмін текстовими повідомленнями та здійснення дзвінків. Був створений компанією SIMCom Wireless Solution, сам модуль реалізований на компоненті SIM900.

Технічні характеристики модуля SIM900:

- діапазон напруг 4,8 – 5,2В;
- у звичайному режимі струм досягає 450 мА, максимальний струм в імпульсному режимі 2 А;
- підтримка 2G;
- потужність передачі: 1 Вт 1800 і 1900 МГц, 2 Вт 850 і 900 МГц;
- вбудовані протоколи TCP і UDP;
- GPRS multi-slot class 10/8;

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35

- робоча температура від -30С до 75 С.

За допомогою даного модуля можна відстежувати маршрут транспорту з GPS приладами. Модуль SIM900 підходить для використання його в охоронних сигналізаціях, але нажаль даний модуль знятий з виробництва та взагалі вважається застарілим. [27]

Опис модуля А6

Модуль А6 використовують для обміну текстовими повідомленнями та даними по GPRS. Даний модуль був розроблений в 2016 році компанією AI-THINKER. Модуль А6 відрізняється від SIM900 малими розмірами та низьким споживанням енергії.

Технічні характеристики модуля А6:

- діапазон напруг 4,5 – 5,5В;
- живлення 5 В;
- діапазон робочих температур від -30С до 80С;
- максимальне споживання струму 900мА;
- GPRS Class 10;
- підтримка протоколів PPP, TCP, UDP, MUX.
- модуль підтримує карти формату мікросім. [27]

Опис модуля А7

Модуль А7 я допрацьованою версію модуля А6 від компанії AI-THINKER. Відмінністю, від свого попередника, є те що модуль А7 має вбудований GPS, що доволі не погано спрощує конструкцію приладу.

Технічні характеристики модуля А7:

- діапазон робочих напруг 3,3 – 4,6 В;
- напруга живлення 5В;
- частоти 850/900/1800/1900 МГц;
- GPRS Class 10: Макс. 85.6 кбіт;

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		36

- придушення луни і шумів.

Даний модуль підтримує не тільки звичайні сім карти, а навіть і мікросім. [27]

На рис. 2.13 показано бездротовий модуль A7 GSM.



Рис 2.13

Опис модуля SIM800L

Даний модуль побудований на основі модуля SIMCom. SIM800L є найчастішим «гостем» у різних проектах де потрібно здійснювати обмін текстовим повідомленням або здійснення виклику на мобільний пристрій. Від своїх попередників модуль SIM800L є доволі простим та дешевим.

Модуль SIM800L має вбудовану антену, що покращує зв'язок. Живити модуль треба через понижуючий перетворювач напруги, адже живиться модуль не від стандартної напруги 3,8 – 4 В.

Технічні характеристики модуля SIM800L:

- діапазон напруг 3,7 – 4,2 В;
- підтримка 4х діапазонної мережі 900/1800/1900 МГц;
- GPRS class 12 (85.6 кБ / с);
- максимальний струм 500 мА;
- підтримка 2G;
- автоматичний пошук в чотирьох частотних діапазонах;
- робоча температура від -30С до 75С. [27]

Проаналізувавши GSM модулі, можна зробити висновок, що доречно використовувати модуль SIM800L. Даний модуль розширює можливості а саме: відправка GPRS, відправлення та отримання текстових повідомлень, здійснювати та отримувати дзвінки. Невелика вартість, невеликі розміри, підтримка частот з 4 діапазонів усе це робить даний модуль ідеальним рішенням для створення охоронної GSM сигналізації.

Після підключення модуля SIM800L к платі Arduino Nano, він починає шукати мобільну мережу та автоматично реєструється. За допомогою вбудованого світлодіода дізнаємося про стан модуля (без знайденої мобільної мережі – швидке мигання, мобільна мережа знайдена – повільне блимання). [20] На рис. 2.14 зображено GSM – модуль SIM800L.

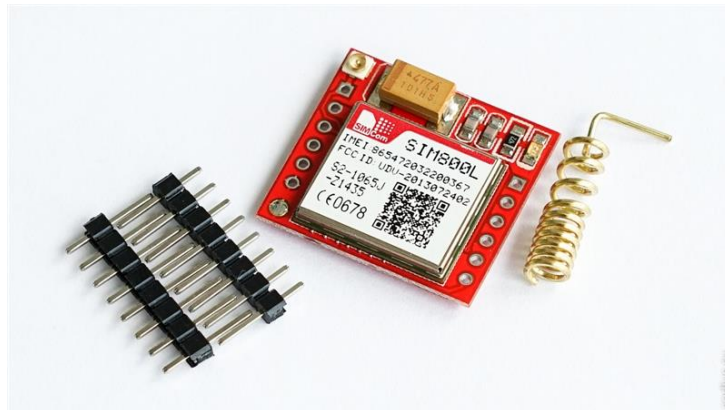


Рис. 2.14

Сам GSM модуль SIM800L знаходиться за металевою кришкою. На рис. 2.15 модуль SIM800L справа на зеленій друкованій платі. [20]



Рис. 2.15

«Сердцем» GSM модуля SIM800L являється чіп Mediatek ARM MT6261. Для GSM / GPRS – зв’язку задає 4 – діапазонний (GSM850 / GSM900 / DCS1800 / PCS1900) приймач RF7198. [20]

MediaTek MT6261 – це така одно кристальна система, яка призначена для першої черги для носіїв електроніки, в основному для розумних годинників, Включає до себе: Bluetooth, LCD, GSM + GPRS, камеру і FM-радіо. На рис. 2.16 зображено чіп Mediatek ARM MT6261 та приймач RF7198. [28]

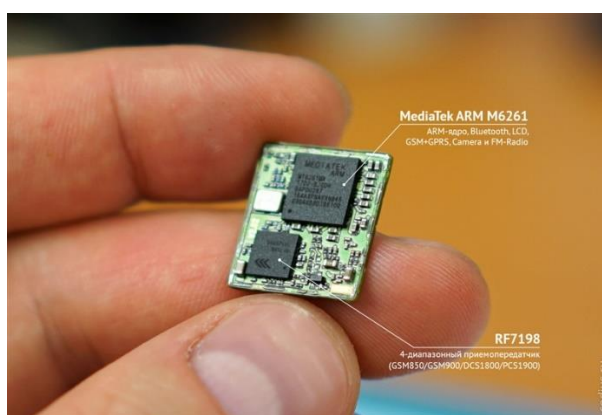


Рис. 2.16

З вище сказаного зрозуміло, що різні модулі серії 800 мають різну характеристику і для остаточного вибору треба провести аналіз їх характеристик і функціоналу. Якщо відкинути несуттєві і однакові для всіх модулів характеристики, то принципові відмінності можна коротко представити у вигляді таблиці.

В табл. 2.17 вказана порівняльна характеристика модулів серії 800. [20]

Всі модулі мають доволі незначні відмінності один з одним. Нам не важлива наявність FM – приймача та Bluetooth, то в принципі можна обрати любий із цієї серії. В даній охоронній сигналізації будемо використовувати GSM модуль SIM800L. [20]

Таблиця 2.17

	SIM800	SIM800	SIM800	SIM800	SIM800	SIM86	SIM80
	0	C	H	L	F	8	8
Голосові виклики	+	+	+	+	+		
GNSS (GPS)						+	+
Bluetooth 3.0	+	+	+				
Вбудований FM-приймач: (76-109 МГц) з кроком 50 кГц			+	+			
CSD	+		+	+			+

Початок роботи з модулем SIM800L

Щоб почати роботу з модулем SIM800L ознайомимося з його функціональною схемою та распиновкою контактів. На рис. 2.18 зображена функціональна схема GSM модуля SIM800L.

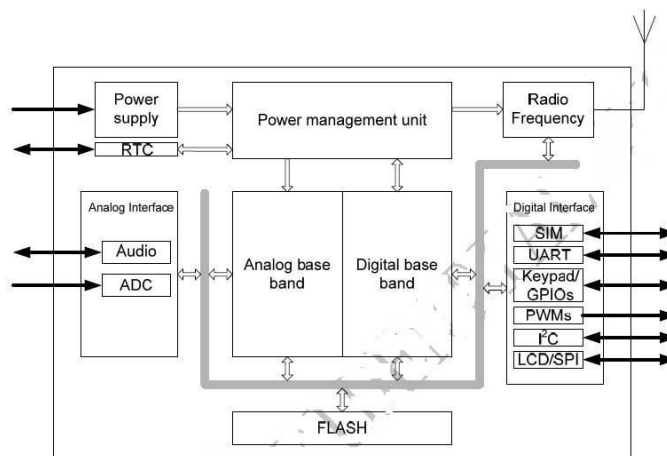


Рис. 2.18

На рис. 2.19 зображено распиновку GSM модуля SIM800L.

Підключення GSM модуля SIM800L к плате Arduino Nano

Наступним кроком після налагодження живлення модуля необхідно підключити відповідні контакти к контактам плати Arduino. Підключати напряду контакти RX, TX не можна. В описі модуля сказано про максимальний рівень логічної одиниці на вході RX яка становить 3,1 В, мінімальна 2,1 В.

На рис. 2.21 вказані характеристики послідовного порту.

Table 10: Serial port characteristics

Symbol	Min	Typ	Max	Unit
V_{IL}	-0.3	-	0.7	V
V_{IH} <i>Input High</i>	2.1	-	3.1	V
V_{OL}	-	-	0.4	V
V_{OH}	2.4	2.8	-	V

Рис. 2.21

На платі Arduino Nano відсутні елементи, що допоможуть конвертувати вхідну напруги навантаження. Тому було прийнято рішення використовувати дільник напруги. Для того щоб організувати потрібний рівень логічної одиниці номіналу 2,5 В необхідно взяти два однакових за номіналом резистора в діапазоні 1 – 10 КОм. На рис. 2.22 наведений приклад дільника напруги та схеми підключення GSM модуля к Arduino Uno із використанням дільника напруги.

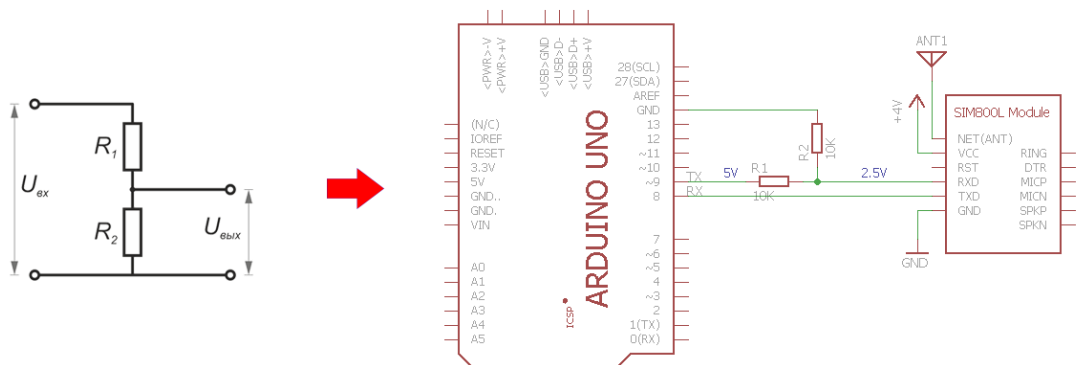


Рис. 2.22

Контакт, на платі Arduino Nano, RX знаходиться в режимі «ВХОДУ», та повністю нормально реагує на логічну одиницю GSM модуля, яка становить 2,8 В. [20]

2.3.3 Вибір датчику відкриття дверей

Усі вимоги, які повинні виконуватися датчиком відкриття дверей задовільнив датчик відкриття дверей МС-38. Даний датчик використовується для оповіщенні відкритті дверей, вікон. У комплекті до датчика відкриття дверей йде безпосередньо сам датчик та магніт, які мають однакову форму. Усередині датчика знаходиться геркон з нормально – розімкнутими контактами. При закритих дверях, коли магніт перебуває близько датчика, контакти датчика замкнені та розмикаються при відкритті дверей. Датчик відкриття можна використовувати для оповіщенні о відкритті дверей, вікон або інших рухомих елементів.

Характеристики датчика відкриття дверей:

- розмір датчик: 27 х 9 х 7 мм;
- розмір магніту: 27 х 9 х 7 мм;
- максимальний струм: 100 mA;
- максимальна напруга: 200 V;
- відстань спрацьовування: від 15 мм до 25 мм;
- в нормальному стані замкнутий;
- спосіб кріплення на шурупи або на клейку ленту;

2.3.4 Вибір п'єзoeлементa

П'єзoeлемент – це електромеханічний перетворювач однією з різновидністю такого п'єзовипромінювача звуку. Частіше його називають п'єзодинаміком або просто дзвінком. Принцип роботи п'єзодинаміка базується на перетворенні електричної напруги в механічні коливання

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		43

мембрани. За допомогою цих коливань створюється те що ми можемо почути – звук.

У обраній моделі п'єзодинаміка частоту звуку можна регулювати програмно задаючи відповідні параметри.

Характеристики п'єзоелементу:

- живлення: 5 В;
- струм: до 30 мА
- частота звуку: 2,3 кГц;
- діаметр: 12мм;
- висота: 9.6мм.

2.3.5 Вибір понижуючого перетворювач напруги

Понижуючий перетворювач напруги (DC – DC перетворювач) – це такий ключ із ШІМ керуванням, до складу якого входить регулятор, що пре значений для регулювання вихідної напруги та струму до відповідного значення, яке буде задовольняти наші вимоги. При виборі понижуючого перетворювача напруги велику увагу звертаємо на діапазон вхідної або вихідної напруги та максимальний вихідний струм.

На сьогоднішній день понижуючий перетворювач напруги задає оптимальне поєднання ефективності, вартості, точності значення на перехідні процеси. На відміну від лінійного регулятора або того ж самого діляника напруги.

Обраний понижуючий перетворювач напруги постійного струму побудований на базі LM2596. Із діапазоном напруги на вході в діапазоні 4,5 – 40 В, на виході 3 – 35 В.

Характеристика понижуючого перетворювача напруги LM2596:

- випрямляч: чи не синхронне випрямлення;
- вхідна напруга: 4.5 – 40 В;
- вихідна напруга: 3 – 35;

- вихідний струм: 2А;
- робочий діапазон температур: -40 ... +85 С;
- захист від короткого замикання: обмеження струму;
- розміри: 44 x 22 x 15 мм.

2.3.6 Вибір резисторів

Резистор – це один із елементів електричного кола, призначений для здійснення опіру електричному струму, тим самим зменшуючи напругу та струм. Одна із основних характеристик резистора являється його величина електричного опору. Лінійна характеристика електричного струму через резистор описується законом Ома:

$$I = \frac{U}{R}; . \quad (2.1)$$

При виборі резисторів враховують наступні вихідні дані:

- номінальна величина опору і допуск на величину опору;
- потужність розсіювання;
- призначення ланцюга, в якій встановлений резистор;
- режим ланцюга: постійний струм, зміни ток або імпульсний режим і, відповідно, сила струму, частота, параметри імпульсів;
- умови експлуатації приладу, температура, вологість, тиск повітря, механічні навантаження;
- бажане конструктивне оформлення резисторів.

Виходячи з вимог та дешевої ціни вибрали підходящий тип резисторів. Резистор 0.125W 220 Ом, 1кОм, 10 кОм які мають характеристику: максимальна потужність (Рмакс), Вт 0.25 та допуск (Δ), 5 ±%.

2.3.7 Вибір конденсаторів

Різні типи конденсаторів зображені на рис. 2.23 і представляють собою двохвивідні компоненти, що використовуються для фільтрації, зберігання

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		45

енергії, придушення імпульсів напруги. У самому простому випадку конденсатори складаються з двох паралельних пластин, що розділені ізоляційним матеріалом (діелектриком).

У найпростішому випадку вони складаються з двох паралельних пластин, розділених ізоляційним матеріалом, званим діелектриком.

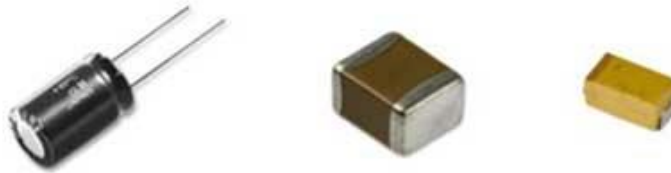


Рис. 2.23

Основна властивість конденсаторів це вміння накопичувати та зберігати електричний заряд. При виборі конденсатора враховуємо наступні параметри:

- робочу напругу конденсатора;
- необхідну точність;
- тип конденсатора;
- робочу температуру;
- спосіб монтажу;

Аналізуючи дані параметри, вибрали конденсатори, які будуть задовільняти всі поставлені нами вимоги. У розробці охоронної сигналізації доцільно використовувати електролітичний конденсатор 2200 мкФ 16 В 105 °С в алюмінієвому циліндричному корпусі, з односпрямованим дротяними гнучкими виводами радіального типу (radial lead). Представлені конденсатори мають полярний тип конструкції. Полярність виводів, номінальну напругу і ємність, а також маркування конденсатора вказані на корпусі за допомогою фарби. Визначити де плюс або мінус конденсатора можна за відмітками на корпусі або по довжині висновків (мінусовий висновок короткий). Допустиме відхилення ємності складає $\pm 20\%$.

2.3.8 Вибір транзисторів та діодів

Транзистор – це напівпровідниковий елемент електронної техніки, який дозволяє керувати струмом, пропускає електричний струм, за допомогою зміни вхідної напруги або струму, поданих на базу, або іншого електрода. Невелика зміна вхідних величин, може призвести до надмірної зміни вихідної напруги та струму.

Діод – це електронний прилад із двома електродами, що випускає електричний струм лише в одному напрямі. Застосовується в багатьох галузях зв'язаних з електронікою .

Транзистори та діоди обрані відповідно до функцій, які вони виконують в схемі. Основними критеріями при цьому були: струм колектора, допустима зворотня напруга та ціна, обрано біполярний транзистор, NPN, 60В, 1,5А, 1,25Вт. Тип корпусу: ТО-126. Виробник: ONS. Та випрямний діод Шотткі; SMD; 30В; 2х6А; DPAK; Упаковка: туба.

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		47

Розділ 3. РОЗРОБКА ДРУКОВАНОЇ ПЛАТИ ПРИСТРОЮ

3.1. Вибір друкованої плати

3.1.1. Вибір типу ДП

Друкована плата, ДП (англ. Printed circuit board, PCB) — пластина, виконана з діелектрика (склотекстоліт, текстоліт, гетинакс, ситал тощо), на якій або всередині якої сформований хоча б один шар з провідними доріжками. На друковану плату монтуються електронні компоненти, які з'єднуються своїми виводами з елементами провідного рисунка паянням, або, значно рідше, зварюванням, у результаті чого складається електронний модуль — змонтована друкована плата [30].

Друковані плати за конструкцією поділяються на такі класи:

- односторонні (одношарові) – ОДП;
- двосторонні (двошарові) – ДДП;
- багатошарові – БДП.

ОДП плата – це друкована плата, що складається з одного шару базового матеріалу або підкладки. Одна сторона основного матеріалу покрита тонким шаром металу. Мідь є найбільш поширеним покриттям через те, що він добре дає собі раду як електричний провідник. Після нанесення мідної основи накладається захисна паяльна маска, за якою може слідувати шар шовкографії, що дозволяє відзначити і підписати всі елементи на платі [31].

ДДП двошарові або двосторонні друковані плати мають базовий матеріал з тонким шаром провідного металу, наприклад, міді, нанесеного на обидві сторони плати. Отвори, просвердлені через плату, дозволяють ланцюгах з одного боку плати підключатися до ланцюгів з другою. Схеми і компоненти двошарової плати зазвичай з'єднуються одним з двох способів: або за допомогою наскрізного отвору, або з використанням поверхневого

монтажу. З'єднання за допомогою наскрізного отвору означає, що через отвори подаються маленькі дроти, відомі як висновки [31].

БДП Багатошарові друковані плати складаються з серії з трьох або більше двошарових друкованих плат. Ці плати потім закріплюються спеціальним клеєм і стають затиснутими між шарами ізоляції, щоб надмірне тепло не розпавило жоден з компонентів. Багатошарові друковані плати бувають різної товщини, зазвичай не менше чотирьох шарів і не більше десяти або дванадцяти шарів. Найбільша багатошарова друкована плата, коли-небудь створена, становила 50 шарів [31].

Згідно із поставленою задачею та схемою електрично принциповою вибираємо ДДП для нашого завдання. Такий вибір зроблений виходячи з аналізу типів ДП. Вибір ДПП дозволяє забезпечити необхідну точність, щільність монтажу, надійність і забезпечити мінімальну вартість.

3.1.2. Вибір матеріалу ДП

Надійсність та працездатність електронного пристрою на пряму залежить від обраного типу матеріалу з якого виготовлена ДП.

При виробництві ДП застосовуються різноманітні матеріали різних виробників. Матеріали, що застосовуються в якості основи для ДП повинні мати:

- високі електроізоляційні властивості;
- достатню механічну міцність;
- бути стійкими до кліматичних впливів.

Цим вимогам задовольняють електротехнічні матеріали: склотекстоліт, кераміка, фторопластова плівка, сапфір і ін.

В даний час одним з основних параметрів є опірність займання. Для цього параметру виділені полімерні композиційні матеріали FR-1 ... FR-5. Найбільш поширеним матеріалом для виробництва ДДП і БДП є FR-4. Стандартний FR-4 представляє собою композитивний матеріал на основі

склотекстоліту. Застосування FR-4 дозволяє отримати отвори високої якості, а це важливо для монтажу елементів.

Таким чином, для реалізації ДДП обраний матеріал FR4-2-35-1,5. Даний матеріал є фольгованим склотекстолітом з підвищеною нагрівостійкістю, товщиною 1,5 мм, покритий з двох сторін мідною електролітичною фольгою товщиною 35 мкм.

3.2 Обґрунтування методу виготовлення ДП

Існують різноманітні методи виготовлення друкованих плат, що відрізняються один від одного поєднанням певного способу нанесення провідників з тим або іншим способом створення провідного покриття. При виборі необхідного методу виготовлення розглянули наступні методи:

- хімічний субтрактивний метод;
- комбінований позитивний метод;
- метод попарного пресування друкованих плат;
- метод пошарового нарощування;
- метод металізації наскрізних отворів.

Кожен з вказаних методів має як переваги, так і недоліки. З урахуванням цих якостей був обраний комбінований позитивний метод. Цей метод полягає в отриманні провідників шляхом труїння фольгованого діелектрика і металізацією отворів електрохімічним способом. Суть методу труїння фольгованого матеріалу з наступним витравленням фольги з окремих ділянок плати. Комбінований позитивний метод забезпечує отримання чітких ліній провідників друкованої схеми. Він характеризується меншою трудомісткістю в порівнянні з електрохімічним методом. Друковані плати надійніші, оскільки при цьому діелектрик знаходиться в сприятливішій умові, тому що фольга оберігає його від дії електроліту.

					ДС52.5217.222.001 ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3 Розрахунок друкованої плати

Визначення мінімальної ширини друкованого провідника

Ширина друкованого провідника по постійному струму позначається літерою b_I розмірність її в мм. Визначення мінімальної ширини друкованого провідника по постійному струмі для ланцюгів живлення та землі визначається за формулою:

$$b_{\min I} = \frac{I_{\max}}{j_{\text{допустиме}} \cdot t_{\text{провідника}}}, \quad (3.1)$$

де I_{\max} – це максимальний струм що може протікати в ланцюгу; $t_{\text{провідника}}$ – це товщина друкованого вузлу; $j_{\text{допустима}}$ – це допустима щільність струму, яка за замовчуванням становить $60 \frac{A}{\text{мм}^2}$.

Товщина друкованого вузла розраховується виразом:

$$t_{\text{провідника}} = h_{\phi} + h_{\text{зм}} + h_{\text{хм}}, \quad (3.2)$$

де h_{ϕ} – це товщина фольги, яка дорівнює 0,035 мм; $h_{\text{зм}}$ – це товщина шара осадженої міді, яка дорівнює 0,055 мм; $t_{\text{провідника}} = 0,035 + 0,055 + 0,0065 = 0,0965$ (мм).

Максимального струму що може протікати в ланцюзі I_{\max} дорівнює сумі усіх струмів, які споживають активні елементи схеми.

$$b_{\min I} = \frac{65 \cdot 10^{-3}}{60 \cdot 0,096} = 0,111 \text{ (мм)}.$$

Отримане значення із розрахунку мінімальної ширини провідника задовольняє четвертий клас точності $b_{\text{прз}} = 0,15$ мм.

Розрахунок мінімальної ширини провідника з урахуванням падіння напруги

Розрахунок мінімальної ширини провідника з урахуванням падіння напруги розраховується

$$b_{\min U} = \frac{\rho \cdot I_{\max} \cdot L_{\text{провідника}}}{U_{\text{доп}} \cdot t_{\text{провідника}}}, \quad (3.3)$$

де ρ – це питомий опір провідника, який дорівнює $0,0175 \frac{\text{Ом} \cdot \text{мм}^2}{\text{м}}$;

$L_{\text{провідника}}$ – це довжина найдового провідника ДП, та дорівнює 0,137 м;

$U_{\text{допустиме}}$ – це допустиме падіння напруги на провіднику;

Розрахунок допустимого падіння напруги на друкованому провіднику здійснюється

$$U_{\text{допустиме}} = 0,05 \cdot E_n, \quad (3.4)$$

$$U_{\text{допустиме}} = 0,05 \cdot 5 = 0,25 \text{ (В)};$$

$$b_{\min U} = \frac{0,175 \cdot 65 \cdot 10^{-3} \cdot 0,137}{0,25 \cdot 0,095} = 65,25 \cdot 10^{-3} \text{ (мм)}.$$

Розрахунок номінального діаметру монтажу отвору

Номінальний діаметр монтажу отвору

$$d_{\text{вс}} + \Delta d_{\text{МО}} + r \leq d, \quad (3.5)$$

де $d_{\text{вс}}$ – це діаметр виводу елементів; $\Delta d_{\text{МО}}$ – це граничне відхилення від номінального діаметру монтажного отвору (МО), та дорівнює 0,1 мм; r – це різниця між діаметром монтажного отвору мінімальним та максимальним значенням виводу елемента, та приблизно дорівнює 0,1 – 0,2 мм.

$$d = 0,5 + 0,1 + 0,2 = 0,8 \text{ (мм)}$$

Розрахунок діаметру контактної площини

Діаметр контактної площини

$$D_{\min} = D_{\min l} + 1,5 \cdot h_{\text{фольги}} + 0,03, \quad (3.6)$$

де $D_{\min l}$ - це мінімальний ефективний діаметр контактної площадки; $h_{\text{фольги}}$ - це товщина фольги, яка дорівнює 0,035 мм.

Коефіцієнт 1,5 треба для врахування підтравлювання фольги друкованого провіднику.

Мінімальний ефективний діаметр контактної площадки

$$D_{\min l} = 2 \cdot (b_{no} + \frac{d_{\max}}{2} + \delta_o + \delta_{\text{км}}), \quad (3.7)$$

де d_{\max} - це максимальне значення діаметру отвору в друкованому провіднику; b_{no} - це ширини пояска контактної площадки, та дорівнює 0.05 мм; δ_o - це похибка розташування центру отвору відносно вузла координатної сітки, та дорівнює 0,07 мм; $\delta_{\text{км}}$ - це похибка розташування центру отвору контактного майданчика відносно вузлу, та дорівнює 0.05 мм.

Максимальний діаметр отвору ДП

$$d_{\max} = d + \Delta d + (0,1), \quad (3.8)$$

де d - це номіральний діаметр монтажного отвору; Δd - це допуск на діаметр отвору, який дорівнює 0,05 мм.

$$d_{\max} = 0,8 + 0,05 + 0,1 = 0,95 \text{ (мм)};$$

$$D_{\min l} = 2 \cdot (0,05 + \frac{0,95}{2} + 0,07 + 0,05) = 1,29 \text{ (мм)};$$

$$D_{\min} = 1,29 + 1,5 + 0,035 + 0,03 = 1,3725 \text{ (мм)}.$$

Максимальний діаметр контактного майданчику

$$D_{\max} = D_{\min} + 0,02; \quad (3.9)$$

$$D_{\max} = 1,3725 + 0,02 = 1,3925 \text{ (мм)}.$$

Розрахунок мінімальної ширини провідника

Мінімальна ширина провідника

$$b_{\min} = b_{np}^{\varepsilon} + 1,5 \cdot h_{\phi} + 0,03, \quad (3.10)$$

де b_{np}^{ε} - це мінімальна ширина провідника, яка визначається з таблиці класів точності.

У даному випадку для четвертого класу точності дорівнює 0,15 мм.

$$b_{\min} = 0,15 + 1,5 + 0,035 + 0,03 = 0,23 \text{ (мм)}$$

Максимальна ширина провідника

$$b_{\max} = b_{\min} + 0,02; \quad (3.11)$$

$$b_{\max} = 0,23 + 0,02 = 0,25 \text{ (мм)}.$$

Розрахунок мінімальної відстані між провідником та контактною площиною

На рис. 3.12 зображено відстань між провідником та контактною площиною.

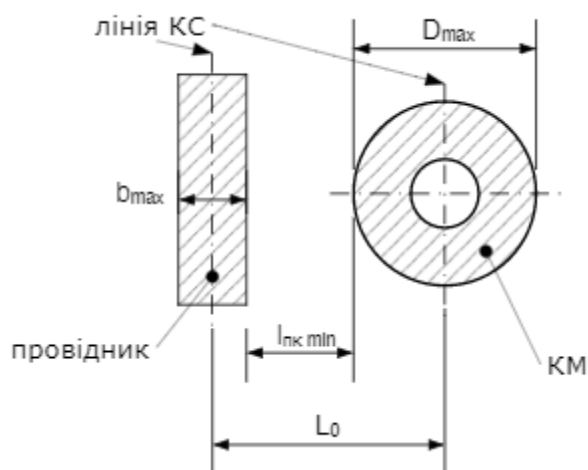


Рис. 3.12

Мінімальна відстань між провідником та контактною площиною

$$l_{ПКМ \min} = L_0 - \left(\frac{D_{\max}}{2} + \delta_{\text{розташування}} + \frac{b_{\max}}{2} + \delta_{\text{зміщення}} \right), \quad (3.13)$$

де L_0 - це відстань між центрами отворів та друкованим провідником, та дорівнює 1,25 мм; D_{\max} - це максимальний діаметр; b_{\max} - це максимальна ширина провідника; $\delta_{\text{розташування}}$, $\delta_{\text{зміщення}}$ - це похибки, які дорівнюють 0,05 мм.

$$l_{ПКМ \min} = 1,25 - \left(\frac{1,39}{2} + 0,05 + \frac{0,25}{2} + 0,05 \right) = 0,33 \text{ (мм)}.$$

Розрахунок мінімальної відстані між двома сусідніми провідниками:

На рис. 3.14 зображено мінімальну відстань між двома сусідніми провідниками

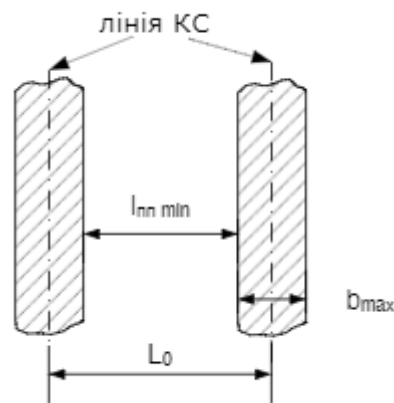


Рис. 3.14

Мінімальна відстань між двома сусідніми провідниками

$$l_{III \min} = L_0 - (b_{\max} + 2 \cdot \delta_{СП}); \quad (3.14)$$

$$l_{III \min} = 1,25 - (0,25 + 2 \cdot 0,05) = 0,9 \text{ (мм)}.$$

Розрахунок мінімальної відстані між двома контактними площинами

На рис. 3.15 зображено мінімальної відстані між двома контактними площинами.

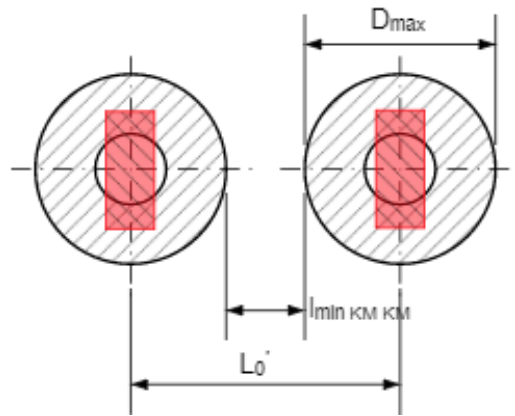


Рис. 3.15

Мінімальна відстань між двома контактними площинами

$$l_{\min KMKM} = L_0 - (D_{\max} + 2 \cdot \delta_{KM}), \quad (3.16)$$

де L_0 - це відстань між центрами сусідніх контактних майданчиків, яка дорівнює 2,5 мм; де L_{01} - відстань між центрами сусідніх КП, $L_{01}=2,5$ мм.

$$l_{\min KMKM} = 2,5 - (1,3925 + 2 \cdot 0,05) = 1 \text{ (мм)}.$$

Розрахунок падіння напруги на найдовшому друкованому провіднику

Падіння напруги на найдовшому друкованому провіднику

$$U = \frac{\rho \cdot I_{\max} \cdot l_{\text{провідника}}}{b_{\text{провідника}} \cdot t_{\text{провідника}}}, \quad (3.17)$$

де ρ - це питомий об'ємний опір, який дорівнює $0,0175 \frac{\text{Ом} \cdot \text{мм}^2}{\text{м}}$; $l_{\text{провідника}}$ - це максимальна довжина друкованого провідника, дорівнює 0,084 мм; $t_{\text{провідника}}$ - це товщина провідника, дорівнює 0,8 мм.

$$U = \frac{0,017 \cdot 3,3 \cdot 0,8}{0,3 \cdot 0,8} = 0,17 \text{ (В)}.$$

Розраховане падіння напруги не перевищує 5% від напруги живлення, що означає добре функціонування приладу.

Розрахунок потужності втрат двосторонньої друкованої плати

Потужність втрат двосторонньої друкованої плати

$$P_{nom} = 2 \cdot \pi \cdot f \cdot C \cdot E_n^2 \cdot tg \sigma, \quad (3.18)$$

де $tg \sigma$ – це тангенс кута діелектричних втрат для матеріала друкованої плати, який дорівнює $tg \sigma = 0,002$ для обраного матеріалу FR4; C – ємність друкованої плати, так, як розрахунок виконується на постійному струмі $f = 1$.

Ємність друкованої плати

$$C = \frac{0,009 \cdot \varepsilon \cdot S_m}{h}, \quad (3.19)$$

де $\varepsilon = 4,5$ – діелектрична проникність для обраного матеріалу FR4; S_m – це площа металізації; h – товщина ДП;

$$C = \frac{0,009 \cdot 4,5 \cdot 500}{1,5} = 13,5 \text{ (нФ)};$$

$$P_{nom} = 2 \cdot 3,14 \cdot 1 \cdot 13,5 \cdot 10^{-9} \cdot 144 \cdot 0,002 = 24,4 \text{ (нВт)}.$$

Розрахунок ємності між двома сусідніми провідниками, які розташовуються на одній стороні ДП

Ємність між двома сусідніми провідниками, які розташовуються на одній стороні ДП та мають однакову ширину

$$C = 0,12 \cdot \varepsilon \cdot l_{\text{провідника}} \cdot \left(\lg \frac{2 \cdot S}{b_{\text{провідника}} + t_{\text{провідника}}} \right)^{-1}, \quad (3.20)$$

де S – це відстань між двома паралельними провідниками; $b_{\text{провідника}}$ – це ширина друкованого провідника; $t_{\text{провідника}}$ – це товщина друкованого провідника; $l_{\text{провідника}}$ – це довжина взаємного перекриття двох паралельних провідників.

$$C = 0,12 \cdot 4,5 \cdot 5 \cdot \left(\lg \frac{2 \cdot 0,9}{0,35 + 0,25} \right)^{-1} = 5,65 \text{ (пФ)}.$$

Розрахунок взаємної індуктивності двох паралельних провідників однакової довжини

Взаємна індуктивність двох паралельних провідників однакової довжини

$$M = 0,02(l_{\text{провідника}} \lg \frac{\sqrt{l_{\text{провідника}}^2 - L_0^2} + l}{L_0} - \sqrt{l_{\text{провідника}}^2 - L_0^2} + l_{\text{провідника}}), \quad (3.21)$$

де $l_{\text{провідника}}$ – це довжина перекриття паралельних провідників; L_0 – це відстань між осевими лініями двох паралельних провідників.

$$M = 0,02(4 \lg \frac{\sqrt{16 - 0,01} + 4}{0,1} - \sqrt{16 - 0,01} + 4) = 1,52 \text{ (нГн)}.$$

Розрахунок середнього часу безвідмовної роботи

Середній час безвідмовної роботи вважається найважливішою мірою надійністю кожного приладу і розраховується таким чином

$$T_{cp} = \frac{1}{\lambda}; \quad (3.22)$$

Інтенсивність відмов елементу є однією із вихідних характеристик надійності приладу. Яка в залежності від кліматичних умов (температура, волога, і т.д.), та режиму роботи.

Інтенсивність відмов елементу

$$\lambda_g = \lambda_{o_3} \cdot K_1 \cdot K_2, \dots, \cdot K_n; \quad (3.21)$$

де λ_{o_3} – це інтенсивність відмов елементу при нормальних умовах роботи (температура навколишнього середовища $T_{\text{окр.ср}} = 20 \pm 5^\circ\text{C}$, відносна вологість повітря $65 \pm 15\%$); $K_1 \cdot K_2, \dots, \cdot K_n$ – це поправочні коефіцієнти, які враховують різні режими роботи та умови експлуатації, $K_n = 1$.

Щоб врахувати вплив режиму роботи приладу на інтенсивність відмови вводять коефіцієнт навантаження, який дорівнює відношенню навантаження в робочому режимі до навантаження в номінальному режимі

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		58

$$K_H = \frac{H_{\text{робоче}}}{H_{\text{номінальне}}}; \quad (3.22)$$

Коефіцієнт навантаження для резисторів

$$K_{н.р} = \frac{P_{\text{робоче}}}{P_{\text{номінальне}}} = \frac{U_{\text{робоче}}^2}{R \cdot P_{\text{номінальне}}}; \quad (3.23)$$

Коефіцієнт навантаження для резисторів

$$K_H = \frac{U_{\text{робоче}}}{U_{\text{номінальне}}}; \quad (3.24)$$

Результуюча інтенсивність відмови дорівнює сумі інтенсивності відмов компонентів

$$\lambda_p = \sum_{i=1}^n \lambda_{pi}; \quad (3.25)$$

$$\lambda_p = \sum_{i=1}^n \lambda_{pi} \approx 1,56 \cdot 10^{-5} (\text{год}^{-1}).$$

Середній час роботи до першої відмови буде дорівнювати:

$$T_{cp} = \frac{1}{1,56 \cdot 10^{-5}} = 64102 (\text{год}).$$

Розрахуємо ймовірність безвідмовної роботи приладу на протязі одного року

$$P = e^{-\lambda_p t}; \quad (3.26)$$

$$P = e^{-1,53 \cdot 10^{-5} \cdot 8760} \approx 0,61.$$

Розрахунок ймовірності відмов на протязі року

$$Q(t) = 1 - 0,61 = 0,39.$$

3.4 Проектування друкованої плати в середовищі EasyEda

EasyEda – це такий сервіс, що дозволяє реалізовувати проекти електронних засобів на рівні схеми з наступною передачею інформації.

Серед автоматизації проектування електроніки включає в себе редактор принципів схем, редактор топології друкованих плат, SPICE-симулятор, хмарне сховище даних, систему управління проектами, а також кошти замовлення виготовлення друкованих плат.

Процес розробки друкованих плат в середовищі EasyEda виконувався в такій послідовності:

1. Створення схеми електричної принципової охоронної сигналізації. Основною панеллю, з якої ведеться робота в редакторі схем, є панель Libraries. EasyEda ділить об'єкти, що знаходяться на полі електричної схеми, на графічні та електричні.

До графічних об'єктів належать:

- лінія;
- дуга, еліптична дуга;
- еліпс, зокрема коло;
- сплайн-крива;
- прямокутник, округлений прямокутник;
- багатокутник;
- секторная діаграма;
- графік.

До електричних об'єктів належать:

- схемні компоненти;
- лінії електричного зв'язку;
- лінії групового зв'язку;
- лінії групового зв'язку у вигляді джгута;
- ідентифікатори ланцюгів.

2. Створення розводки друкованої плати. Створення файлу плати може бути виконано вручну. У EasyEda виконується завдання інтерактивного трасування вирішується інструментом автотрасування розташованим в меню AutoRoute. Автоматичне трасування окремих елементів дає не дуже

					ДС52.5217.222.001 ПЗ	Арк.
						60
Змн.	Арк.	№ докум.	Підпис	Дата		

задовільний результат, тому що немає можливості настройки її алгоритму, який може бути зазначений тільки для трасування всієї плати. На рис. 3.1. зображено трасування ДП охоронної GSM сигналізації.

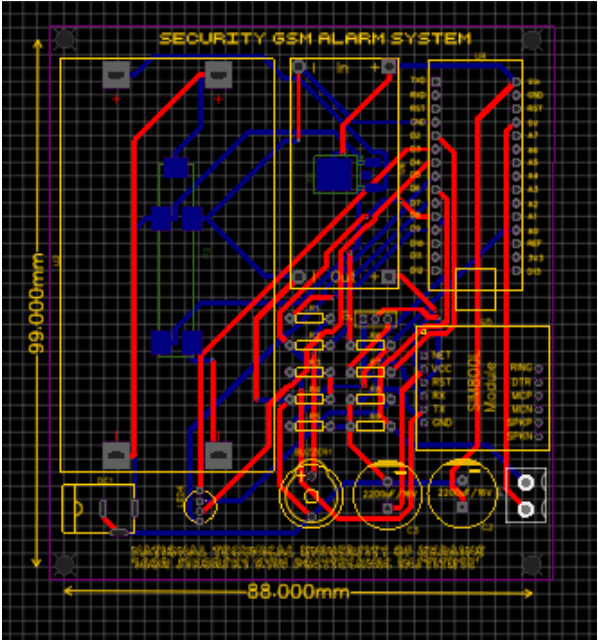


Рис. 3.1

Розділ 4. РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

4.1 Моделювання програмного забезпечення

Для створення якісного програмного забезпечення, треба провести якісний аналіз та моделювання програмного забезпечення. Для моделювання програмного забезпечення використаємо методологію створення діаграм BPMN (Business Process Model and Notation).

Модель і нотація бізнес-процесів (BPMN, Business Process Model and Notation) - методологія моделювання, аналізу і реорганізації бізнес-процесів. Основною метою BPMN є забезпечення доступної нотацією опису бізнес-процесів всіх користувачів: від аналітиків, що створюють схеми процесів, і розробників, відповідальних за впровадження технологій виконання бізнес-процесів, до керівників і звичайних користувачів, які керують цими бізнес-процесами і відстежують їх виконання. Таким чином, BPMN націлений на усунення розбіжності між моделями бізнес-процесів і їх реалізацією [29].

На рис. 4.1 зображено процес увімкнення охоронної сигналізації.

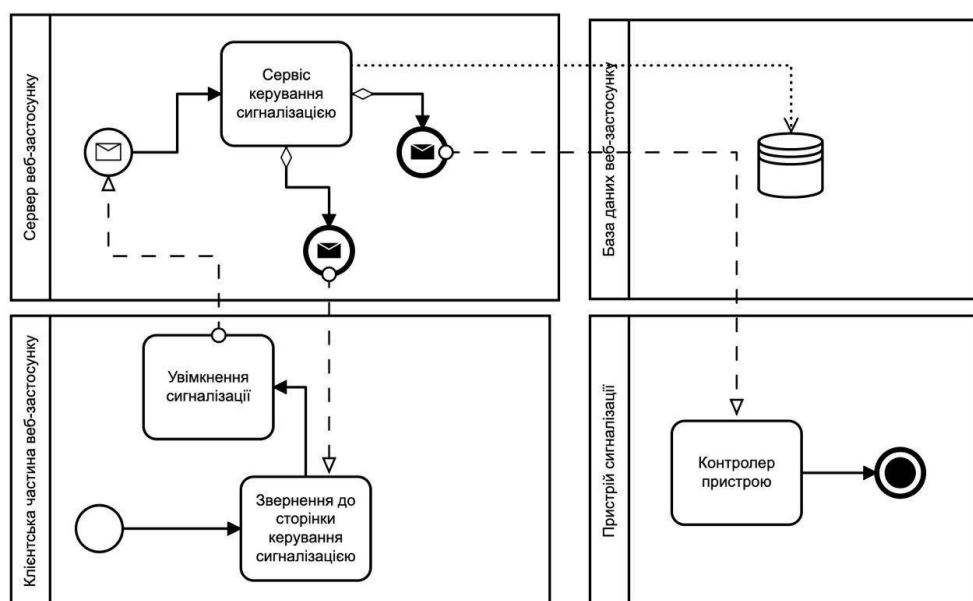


Рис. 4.1

Детальний опис процесу увімкнення охоронної сигналізації:

Опис процесу увімкнення сигналізації:

- користувач звертається до сторінки керування сигналізацією;
- натискає на кнопку увімкнення сигналізації;
- відправляє на сервер запит на вмикання;
- сервіс керування сигналізацією перевіряє з'єднання з пристроєм та надсилає запит на вмикання сигналізації контролеру пристрою;
- якщо пристрій під'єднаний, то сигналізація успішно вмикається;
- інакше сервіс повідомляє користувача, що пристрій не під'єднано, повертаючи на сторінку керування сигналізацією.

На рис. 4.2 зображено процес вимкнення охоронної сигналізації.

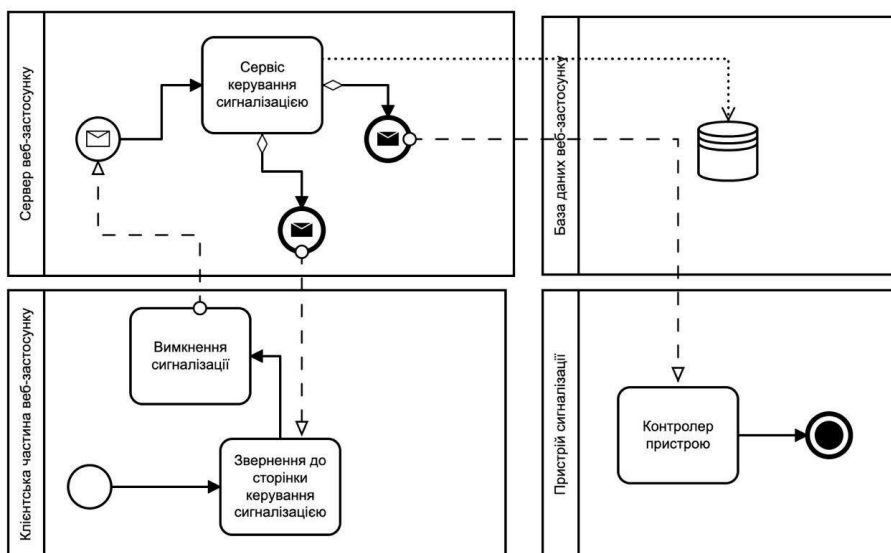


Рис. 4.2

Детальний опис процесу увімкнення охоронної сигналізації:

- користувач звертається до сторінки керування сигналізацією;
- натискає на кнопку вимкнення сигналізації;
- відправляє на сервер запит на вимикання;
- сервіс керування сигналізацією перевіряє з'єднання з пристроєм та надсилає запит на вимикання сигналізації контролеру пристрою;
- якщо пристрій під'єднаний, то сигналізація успішно вимикається;

- інакше сервіс повідомляє користувача, що пристрій не під'єднано, повертаючи на сторінку керування сигналізацією.

4.2 Програмування контролеру Atmega328P

Програмування контролеру було виконано за допомогою програми Arduino IDE, так як там присутні зручні бібліотеки для роботи з UART та I2C інтерфейсом, а також це спрощує саме програмування контролеру.

У ході виконання роботи було створено програму, за допомогою якої охоронна GSM сигналізація працює автоматично. Програмний код охоронної сигналізації представлений у Додатку Б.

Розроблювальну програму можна розділити на 3 частини:

- зчитування показників з датчиків;
- автоматична робота пристрою;

Для управління даною охоронною сигналізацією було написано сервер за допомогою мови програмування Java. Також управляти охоронною сигналізацією можна за допомогою текстових повідомлень, які можна надсилати зі свого смартфона.

Після встановлення на охорону система оповістить про успішність встановлення та засвітить світлодіод зеленим кольором.

Функція охоронної систем реалізована за допомогою датчику відкриття дверей (магніт та геркон). Якщо охорона система спрацює (при відкритті дверей під час включеної охоронної системи), на мобільний телефон, номер який буде указано в програмі прийде текстове повідомлення з текстом «Alarm! Door open» та динамік почне випромінювати звук типу сирени, світлодіод змінить свій колір світіння. Алгоритм роботи представлений у Додатку В.

4.3 Тестування програмного забезпечення

У такому складному та величезному процесі, як розробка програмного забезпечення, тестування є найголовнішим етапом. Люди часто не звертають достатньо уваги. Всі допускають, що готова система буде працювати ідеально за усіма вимогами, але не завжди програмне забезпечення написано ідеально.

Визначивши важливість тестування програмного забезпечення, який є одним із найважливіших етапів розробки. У рамках плану тестування буде виконано тестування основної частини системи. У плані тестування програмного забезпечення буде перевірено наступні функції:

- створення користувачів;
- авторизація користувачів;
- увімкнення сигналізації;
- вимкнення сигналізації;
- спрацювання сигналізації.

Тестування програмного забезпечення будемо здійснювати наступними методами:

- компонентне;
- інтеграційне;
- системне.

Компонентне тестування програмного забезпечення

Методом компонентного тестування будуть перевірені наступні частини застосунку:

- сервісні методи для створення та видалення користувачів;
- методи авторизації.

Для компонентного тестування критерієм проходження є успішне виконання кожного пункту тесту. У разі якщо хоча б один пункт не був успішно виконаний – тестування вважається не пройденим.

					ДС52.5217.222.001 ПЗ	Арк.
						65
Змн.	Арк.	№ докум.	Підпис	Дата		

Інтеграційне тестування програмного забезпечення

Методом інтеграційного тестування будуть перевірені взаємодії між модулями системи, такі як:

- взаємодія веб-сервера з базою даних;
- взаємодія веб-сервера з застосунком адаптером.

Для інтеграційного тестування критерієм проходження є успішне виконання кожного пункту тесту. У разі якщо хоча б один пункт не був успішно виконаний – тестування вважається не пройденим [30].

Системне тестування програмного забезпечення

Методом системного тестування буде перевірено взаємодію найголовніших елементів системи:

- вмикання сигналізації на пристрою;
- вимикання сигналізації на пристрою;
- спрацювання сигналізації на пристрою.

Для системного тестування необхідно підключити всі елементи системи та перевірити їх повну взаємодію на коректність поведінки. Тестування вважається пройденим, якщо всі основні сценарії виконуються з очікуваними результатами [30].

Тестування програмного забезпечення охоплює низку видів діяльності, дуже аналогічний послідовності процесів розробки програмного забезпечення. Сюди входять завдання для тесту, проектування, написання тестів, тестування тестів і, нарешті, виконання тестів вивчення результатів тестування. Вирішальну роль грає проектування тесту. Можливий цілий спектр підходів до розробки філософії, чи стратегії проектування тестів [30].

ВИСНОВКИ

За результатами дипломного проекту було спроектовано та розроблено охоронну GSM сигналізацію. Дана сигналізація є універсальною керувати сигналізацію можна за допомогою мобільного пристрою або серверу. Даний пристрій може впевнено зайняти нішу проектів «охоронних GSM сигналізацій», оскільки на ринку України таких пристроїв не так й то і багато, а з аналогами, пристрій буде конкурувати за рахунок цінових показників.

У відповідності до розробленої схеми електричної структурної пристрою було проведено вибір елементної бази, опис роботи та підключення структурних блоків. На основі цих даних спроектовано схему електричну принципову та перелік елементів.

Проведена конструкторська та технологічна розробка ДП, в ході якої було прийнято рішення виконати друкований вузол на двосторонній друкованій платі зі склотекстоліту, обґрунтовано спосіб виготовлення ДП.

Для виконання друкованої плати використовуємо двухсторонній текстоліт FR-2-35-1.5. Обґрунтовано вибір виготовлення плати комбінованим позитивним методом. Для конструювання обрано 4-й клас точності, так як він забезпечує достатню щільність монтажу з урахуванням потрібних нам габаритів пристрою.

На основі проведеної роботи розроблено друкований вузол в середовищі EasyEda. Креслення оформлені за допомогою САПР Autodesk AutoCAD.

Також розроблено алгоритм програми для мікроконтролеру та написано програму для нього у середовищі Arduino IDE, які представлені у додатку Б та В відповідно. Окрім цього, розроблено сервер, що формує команди та відправляє їх по кабелю, спроектованій охоронній сигналізації.

					ДС52.5217.222.001 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		67

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. <http://www.vide.com.ua/alarm/gsm/>
2. <http://www.vide.com.ua/documents/gsm-signalizacia-hto-eto/>
3. http://asupro.com/building/security/peripheral-devices-security-fire-systems.html?utm_source=www.google.com
4. <https://www.lankey.ru/engineering/bezopasnost/867/871/>
5. Елементи Радіоелектронної Апаратури. Випуск 26. Стальбовскій В.В., Четвертков І.І. Резистори. Москва: Видавництво «Радянське радіо», 1973 рік.
6. <http://www.firma-rubezh.com.ua/30>
7. <https://ru.wikipedia.org/wiki/%D0%9C%D0%B8%D0%BA%D1%80%D0%BE%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D0%BB%D0%B5%D1%80>
8. Терещенко Т. О., Тодоренко В. А., Батрак Л. М., Ямненко Ю. С. Мікропроцесорні пристрої: Навчальний посібник для студентів спеціальності «Електроніка». - К.: КПІ ім. Ігоря Сікорського, 2017. – 244 с.
9. Опис мікроконтролерів PIC16C7X. Web Site: [http:// www. microchip.com](http://www.microchip.com).
10. Опис мікроконтролерів Atmega. - WebSite: [http:// www. atmel.com](http://www.atmel.com).
11. Одно кристальний мікроконтролери Microchip: PIC16C5X. Під ред. А.Н. Владимірова. - М: ORMIX, 1996. - 96 с.
12. <http://robolive.ru/mikrokontroller-atmega328-opisanie-xarakteristiki/>
13. https://arduinomaster.ru/platy-arduino/plata-arduino-nano/#_Arduino_Nano
14. <http://www.electronica52.in.ua/proekty-arduino/raspinovki-processorov-atmega-i-atini->
15. https://ru.wikipedia.org/wiki/%D0%A2%D0%B8%D0%BF%D1%8B_%D0%BA%D0%BE%D1%80%D0%BF%D1%83%D1%81%D0%BE%D0%B2

_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D1%80%D0%BE%D0%B2#QFP

16. Бєлов А.В. - Мікроконтролери AVR в радіоаматорського практиці, 2007. – 352 с.

17. <https://arduinoplus.ru/arduino-nano/>

18. https://arduino-master.ru/platy-arduino/plata-arduino-nano/#_Arduino_Nano

19. <http://elektrik.info/main/praktika/1112-dcdc-preobrazovateli.html>

20. http://codius.ru/articles/GSM_%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C_SIM800L_%D1%87%D0%B0%D1%81%D1%82%D1%8C_1

21. <https://txcom.ru/ohrannaya-signalizaciya>

22. <http://pbsecurity.ru/obzoryi-i-rekomendatsii/izveschateli-ohrannoy-signalizatsii.-detektoryi-dvizheniya.html>

23. <http://www.bre.ru/security/25144.html>

24. <http://microsin.net/programming/avr/difference-between-atmega328p-and-atmega328.html>

25. <https://arduinoplus.ru/arduino-ide-opisanie-gde-skachat/>

26. <https://ru.wikipedia.org/wiki/GSM>

27. <https://arduino-master.ru/datchiki-arduino/gsm-gprs-modul-arduino/>

28. <https://mediatek-club.ru/mediatek-mt6261>

29. https://sites.google.com/site/anisimovkhv/learning/pris/lecture/tema8/tema8_4

30. https://uk.wikipedia.org/wiki/%D0%94%D1%80%D1%83%D0%BA_%D0%BE%D0%B2%D0%B0%D0%BD%D0%B0_%D0%BF%D0%BB%D0%B0%D1%82%D0%B0

31. <http://digitrode.ru/articles/1232-kakie-vidy-pechatnyh-plat-suschestvuyut.html>

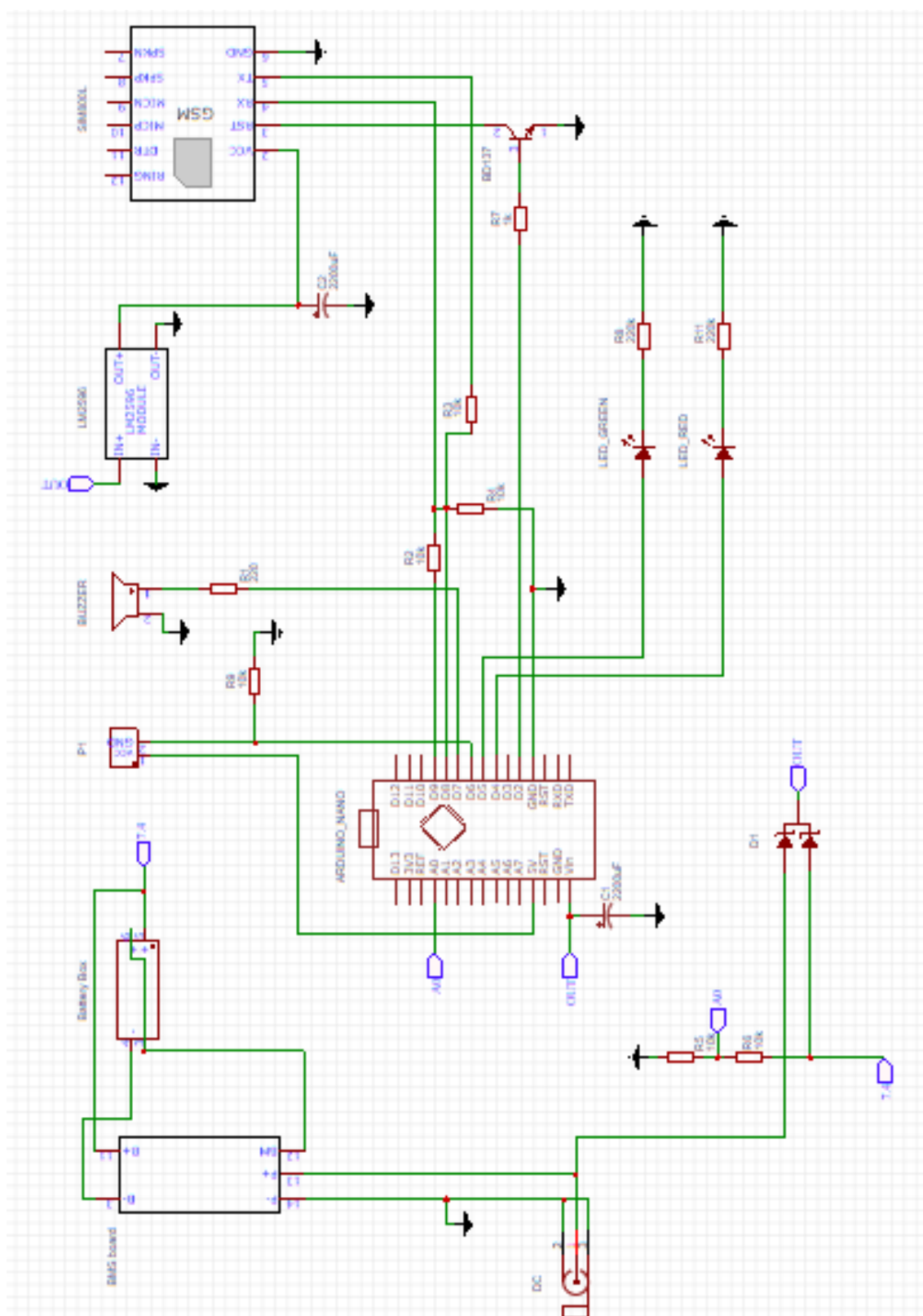
Позначення	Найменування	Кількість	Примітки
	<u>Деталі</u>		
1	Схема електрична	1	
	<u>Конденсатори</u>		
2	ЕСАР (К50-35) 2200 мкф, 16В	2	С1, С2
	<u>Модулі</u>		
3	SIM800L	1	GSM
4	Arduino Nano	1	MCU
5	LM2596	1	DC-DC
	<u>Світлодіоди</u>	1	С3
6	Світлодіод червоний 5 мм	1	HL1
7	Світлодіоді зелений 5 мм	1	HL2
	<u>Роз'єми</u>		
8	KF-301-500-2P Kefeng	1	XP1
	<u>Резистори</u>		
9	0.125-220Ом±5%	3	R8,R10,R1
10	0.125-1kОм±5%	1	R7
11	0.125-10kОм±5%	6	R2, R3, R4, R5, R6, R9
	<u>Транзистори</u>		
12	BD137 STMicroelectronics	1	VT1
	<u>Матеріали</u>		
13	Пріпій ПОС-61 ГОСТ 21930-76	30г	

					ДС52.5217.222.001 ПЕЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Схема електрична принципова Перелік елементів	Літ.	Арк.	Аркушів	
Розробив	Саларов М.М.						1	2	
Перевірів	Бондаренко О.Ф..								
Н. Контр.	Батрак Л.М.					КПІ ім. Ігоря Сікорського, ФЕЛ, КПЕ, гр. ДС-52			
Затвердив	Бондаренко О.Ф..								

Змн.	Арк.	№ докум.	Підпис	Дата

Арк.
2

Додаток А



Додаток Б

```
#include <EtherCard.h>
#include <SoftwareSerial.h> //
Бібліотека програмної реалізації обміну по UART-протоколу
SoftwareSerial SIM800(8, 9); // RX, TX

// ethernet інтерфейс mac address, повинен бути унікальним
в локальній мережі
static byte mymac[] = { 0x74,0x69,0x69,0x2D,0x30,0x31 };

byte Ethernet::buffer[700];
static uint32_t timer;

const char website[] PROGMEM = "192.168.0.104";
static byte websiteip[] = { 192,168,0,104 };
static byte myip[] = { 192,168,0,114 };
BufferFiller bfill;
boolean protection = false;
boolean wasSent = false;

int green = 4; // контакт для зеленої індикації
int red = 5; // контакт для червоної індикації

int Door_Sensor_Pin = 6; // контакт для датчика
int buzzer = 7; // контакт для «сирени»
int val = 0; // змінна для зберігання стану датчика

// виклик при завершенні запиту клієнта
static void my_callback (byte status, word off, word len) {
    Serial.println(">>>");
    Ethernet::buffer[off+300] = 0;
    Serial.print((const char*) Ethernet::buffer + off);
```

```

        Serial.println("...");
    }

    void sendSMS(String phone, String message)
    {
        sendATCommand("AT+CMGS=\"" + phone + "\"",
true);        // Переходимо в режим введення тексту повідомлення
        sendATCommand(message + "\r\n" + (String)((char)26),
true);        // Після тексту відправляємо перенесення рядка і Ctrl +
Z}

    static word homePage() {
        long t = millis() / 1000;
        word h = t / 3600;
        byte m = (t / 60) % 60;
        byte s = t % 60;
        bfill = ether.tcpOffset();
        bfill.emit_p(PSTR(
            "HTTP/1.0 200 OK\r\n"
            "Content-Type: text/html\r\n"
            "Pragma: no-cache\r\n"
            "\r\n"
            "<meta http-equiv='refresh' content='1'/>"
            "<title>RBBB server</title>"
            "<h1>$D$D:$D$D:$D$D</h1>"),
            h/10, h%10, m/10, m%10, s/10, s%10);
        return bfill.position();
    }

    String sendATCommand(String cmd, bool waiting) {
        String _resp = "";                                // Змінна
        для зберігання результату                        Serial.println(cmd);
        // Дублюємо команду в монитор порта
        SIM800.println(cmd);                                //

```



```

Відправляємо команду модулю
    if (waiting) {                                     // Якщо
необхідно дочекатися відповіді ...
        _resp = waitResponse();                         // ...
чекаємо, коли буде переданий відповідь
        // Якщо Echo Mode вимкнений (ATE0), то ці 3 рядки можна
закоментувати
        if (_resp.startsWith(cmd)) {                   //
Прибираємо з відповіді дублює команду
            _resp = _resp.substring(_resp.indexOf("\r",
cmd.length()) + 2);
        }
        Serial.println(_resp);                         // дублюємо
відповідь в монітор порту
    }
    return _resp;                                       //
Повертаємо результат. Пусто, якщо проблема
}

String waitResponse() {                               // Функція
очікування відповіді і повернення отриманого результату
    String _resp = "";                                 // Змінна
для зберігання результату
    long _timeout = millis() + 10000;                 // Змінна
для відстеження таймаута (10 секунд)
    while (!SIM800.available() && millis() < _timeout)
    {}; // Чекаємо відповіді 10 секунд, якщо прийшла відповідь або
настав таймаут, то ...
    if (SIM800.available()) {                         // Якщо є,
що зчитувати ...
        _resp = SIM800.readString();                 // ...
зчитуємо і запам'ятовуємо
    }
    else {                                             // Якщо

```

```

    прийшов таймаут, то ...
        Serial.println("Timeout...");                // ...
    сповіщаємо про це і ...
    }
    return _resp;                                     // ...
    повертаємо результат. Пусто, якщо проблема
}

String _response = "";

void setup () {
    Serial.begin(9600);
    SIM800.begin(9600);

    sendATCommand("AT", true);
    _response = sendATCommand("AT+CMGF=1;&W", true);
    Serial.println(F("\n[webClient]"));

    pinMode(Door_Sensor_Pin, INPUT);
    pinMode(buzzer, OUTPUT);
    pinMode(red, OUTPUT);
    pinMode(green, OUTPUT);
    delay(3000);
    digitalWrite(green, HIGH);
    digitalWrite(red, HIGH);
    delay(3000);
    if (ether.begin(sizeof Ethernet::buffer, mymac) == 0)
        Serial.println(F("Failed to access Ethernet
controller"));
    if (!ether.dhcpSetup())
        Serial.println(F("DHCP failed"));

    ether.staticSetup(myip);

```

```

ether.printIp("IP: ", ether.myip);
ether.printIp("GW: ", ether.gwip);
ether.printIp("DNS: ", ether.dnsip);

if (!ether.dnsLookup(website))
    Serial.println("DNS failed");
memcpy(ether.hisip, websiteip, sizeof(websiteip));
ether.printIp("SRV: ", ether.hisip);
ether.hisport = 8080;
}

void loop () {
    word len = ether.packetReceive();
    word pos = ether.packetLoop(len);

    if (pos) { // check if valid tcp data is received
        char* data = (char *) Ethernet::buffer + pos;
        Serial.println(data);
        char *pCh = strstr(data, "enable");
        char *pCh2 = strtok (pCh, " &");
        // в другому параметрі вказані роздільники (пропуск,
кома, точка)
        if (strcmp(pCh2, "enable=true") == 0) {
            protection = true;
            digitalWrite(green, HIGH);
            digitalWrite(red, LOW);
        } else if (strcmp(pCh2, "enable=false") == 0) {
            protection = false;
            digitalWrite(green, LOW);
            digitalWrite(red, LOW);
        }
        ether.httpServerReply(homePage());
    }
}

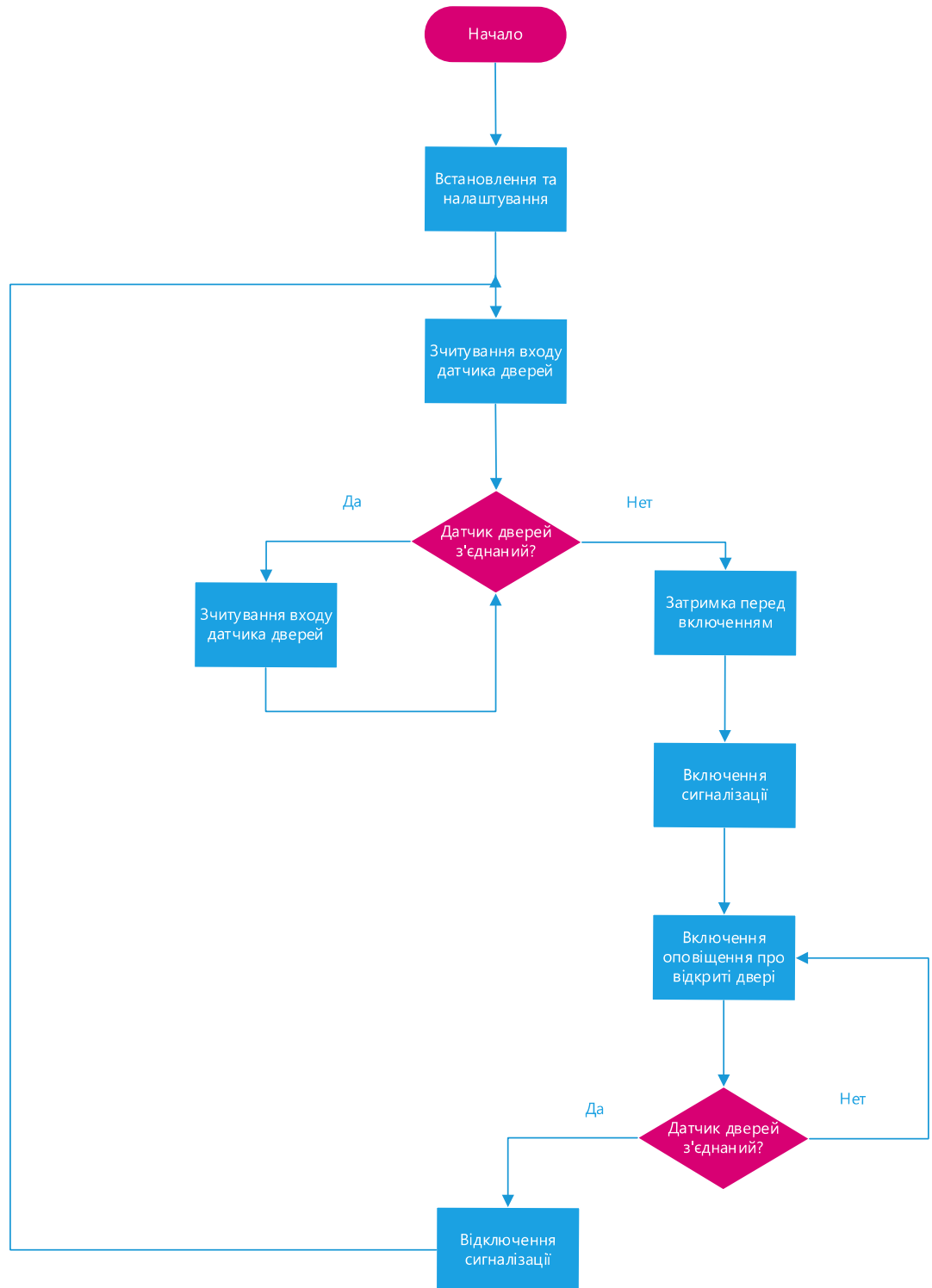
```

```

        val    =    digitalRead(Door_Sensor_Pin);    //    читати
Door_Sensor_Pin
        if (protection == true && val == LOW) { // Якщо
Door_Sensor N.C. (Без магніту) -> HIGH: Двері відчинені / LOW:
Двері закриті
            digitalWrite(buzzer, HIGH);
            digitalWrite(green, LOW);
            digitalWrite(red, HIGH);
        //                                ether.browseUrl(PSTR("/warning?"),
"warning=warning", website, my_callback);
            if (wasSent == false) {
                sendSMS("+380956275355", "WARNING");
                wasSent = true;
            }
        } else {
            digitalWrite(buzzer, LOW);
            if (protection == true) {
                digitalWrite(green, HIGH);
                digitalWrite(red, LOW);
            } else {
                digitalWrite(green, LOW);
                digitalWrite(red, LOW);
            }
            wasSent = false;
        }
    }
}

```

Додаток В



Додаток Г

Abstract

The object of research and development is a security alarm system with a GSM module.

In this diploma project, a security alarm system with a GSM module was designed and developed. This device must perform the following basic functions: connecting and monitoring the status of various sensors (fire safety, presence, etc.) sending messages to the owner of the GSM - signaling about the wrongful penetration of the home.

The signaling must have input and output enforcement organs where the input is used to activate, for example, any loop of the alarm or its deactivation, the outputs can be used to turn on sirens and many others.

To design the system of premises security, it was decided to implement this device on the basis of Arduino Nano MK. The transmission of information will be realized by means of GSM communication, considering that the wired security systems are not reliable. Also, the GSM connection automatically makes the device independent of electricity or Wi-Fi. The SIM800L module will help you establish a GSM connection between our devices and our mobile operator.

After the analytical review, the calculations have been designed optimized and most importantly not expensive cost alarm system. The respective components of the card were purchased, the device was assembled and software code was written. The result was a ready-to-sell alarm system for the premises, and not only.

GSM Based Home Security Alarm System Using Arduino

Home Security Systems are an important feature of modern residential and office setups. Home security systems must be affordable, reliable and effective.

Modern complex home security systems include several security features like fire, intruders, electronic door lock, heat, smoke, temperature, etc. Some security systems may be a combination of all the security measures.

Such complex systems may be expensive and may not be affordable by everyone. There are individual security systems based on the requirement.

In this project, we designed a simple but very efficient home security that has a function of calling the homeowner on his/her mobile number in case of an intruder alert.

The project is based on Arduino, PIR motion detection sensor and GSM Module.

Circuit Design of Arduino GSM Home Security Alarm System

As the project is based on an Arduino, the connection is pretty simple. PIR motion detection sensor module has a digital output pin. This is connected to any of the digital I/O pins of the Arduino.

The GSM Module communicates with the microcontroller in a serial manner. It has an Rx and Tx pins on the board. These pins are connected to the Tx and Rx pins of the Arduino.

It is important to note that while uploading the program (sketch) to Arduino, the GSM module must be disconnected as it might interfere with the serial communication with the Arduino IDE.

Component Description

PIR Motion Detection Sensor

Passive Infra-Red or PIR Sensor is a Pyroelectric device that detects motion. Hence, it is also called as motion detection sensor. It detects motion by sensing the changes in infrared levels emitted by nearby objects.

GSM Module

SIM 800L is the GSM/GPRS module with built in RS232 interface. It has dual band GSM/GPRS system that works on 900/1800MHz frequencies.

With the help of RS232, the modem can be connected to PC or microcontroller via serial cable. Voice calls, SMS and internet access are possible with this module.

There are on board connections for microphone and headphones with which we can make or receive calls.

Arduino Nano

It is the main controller used in this project. It detects the signals from PIR sensor and sends commands to GSM Module accordingly. The serial pins of the Arduino are used in this project to communicate with GSM module.

Working of Arduino GSM Home Security Alarm System

Home Security Alarm Systems are very important in present day society, where crime is increasing. With the technological advancements we have achieved in the recent years, a homeowner doesn't have to worry about home security while getting off his/her home.

Modern home security systems provide enough security from burglars, fire, smoke, etc. They also provide immediate notification to the homeowner.

The aim of this project is to implement a simple and affordable, but efficient home security alarm system. The project is designed for detecting intruders and informing the owner by making a phone call.

The working of the project is explained below.

PIR sensor detects motion by sensing the difference in infrared or radiant heat levels emitted by surrounding objects. The output of the PIR sensor goes high when it detects any motion. The range of a typical PIR sensor is around 6 meters or about 30 feet.

For proper operation of PIR sensor, it requires a warm up time of 20 to 60 seconds. This is required because, the PIR sensor has a settling time during which it calibrates its sensor according to the environment and stabilizes the infrared detector.

During this time, there should be very little to no motion in front of the sensor. If the sensor is not given enough calibrating time, the output of the PIR sensor may not be reliable.

When the PIR sensor detects any motion, the output of the sensor is high. This is detected by the Arduino. Arduino then communicates with the GSM

module via serial communication to make a call to the pre programmed mobile number.

An important point to be noted about PIR sensors is that the output will be high when it detects motion. The output of the sensor goes low from time to time, even when there is motion which may mislead the microcontroller into considering that there is no motion.

This issue must be dealt with in the programming of Arduino by ignoring the low output signals that have a shorter duration than a predefined time. This is done by assuming that the motion in front of PIR sensor is present continuously.

According to the results of the diploma project, a guarded GSM alarm system was designed and developed. This alarm is a universal signaling system managed by a mobile device or server. This device can confidently occupy a niche of "guarded GSM alarm systems" projects, as there are not so many such devices in the Ukrainian market, and with the analogues, the device will compete at the expense of price indicators.

In accordance with the developed scheme of the electrical structural unit, the choice of the element base, the description of the work and the connection of structural blocks were made. On the basis of these data, the design of the electric principle and the list of elements is designed.

The design and technological development of the State Enterprise was carried out, during which it was decided to execute the printed knot on a double-sided printed circuit board from a glass fiber reinforced fabric, and the method of manufacturing the AP was substantiated.

To perform the printed circuit board, use the two-sided text-lead FR-2-35-1.5. The choice of making a board with a combined positive method is substantiated. For designing, the 4th grade of precision is chosen, since it provides a sufficient density of installation, taking into account the dimensions of the device we need.

On the basis of the work, the printhead was developed in the EasyEda environment. Drawings are executed using Autodesk AutoCAD CAD.

An algorithm for the program for the microcontroller is also developed and the program for it in the Arduino IDE environment, which is presented in note B and B, is written accordingly. In addition, a server has been developed that generates commands and sends them on a cable designed with a security alarm system.